Instituto Universitário de Lisboa

Escola de Tecnologia e Arquitectura
Departamento de Ciências e Tecnologias da Informação

"Combater o Crime Económico com Armas Digitais: O Papel do Open-Source"

Manuel Delgado

Dissertação submetida como requisito parcial para obtenção do grau de
Mestre em Open Source Software

Orientador:
Doutor Carlos J. Costa, Professor Auxiliar,
ISCTE-IUL

Co-orientadora:
Mestre Manuela Aparício,
Adetti-ISCTE

Abril 2012

AGRADECIMENTOS

Podemos fixar um objectivo por iniciativa própria, mas muito dificilmente o concretizamos isoladamente.

Lancei-me nesta aventura por impulso. Ao terminar, constato que nada teria concretizado sem o apoio de terceiros.

Resta-me pois, registar o meu profundo apreço a todos quantos, de diferentes formas, me apoiaram na concretização de mais este objectivo, endereçando o meu especial agradecimento:

À minha família, em particular a minha esposa e filho, que sempre me apoiaram, pelas inúmeras ausências e reduzida atenção a que os votei, ao longo deste ano e meio;

Aos meus orientadores, Doutor Carlos Costa e Mestre Manuela Aparício, por terem acreditado na minha proposta de trabalho e por todo o incentivo e auxílio na superação dos inúmeros desafios encontrados, pelo empenho com que orientaram este trabalho nas diversas fases, pelo rigor e pela oportunidade das críticas e sugestões;

Aos colegas da turma do MOSS 2010/2012, pela excelente camaradagem e pelo muito que convosco aprendi;

Finalmente, um imenso agradecimento aos restantes familiares, colegas de trabalho e amigos que compreenderam e suportaram tantas ausências decorrentes de todas as obrigações e compromissos associados a esta empreitada.

RESUMO

A par do extraordinário desenvolvimento económico proporcionado pela evolução das Tecnologias da Informação e Comunicação, potenciado, nos anos mais recentes, com o desenvolvimento da internet, consolida-se uma dimensão anárquica e obscura que, a coberto do anonimato e tirando partido da mesma tecnologia, veicula uma miríade de comportamentos de natureza criminosa, que tendem a subverter os princípios básicos da vivência em sociedade, alguns dos quais, contribuíram em larga medida para a dimensão da presente crise económica.

Grande parte das dificuldades que a generalidade dos sistemas de justiça enfrentam, para dominar este novo tipo de criminalidade, radicam no *Gap* Tecnológico que se verifica nas tecnologias de que dispõe, face aos meios utilizados pelo crime organizado.

Tomando como referencial o fenómeno do crime económico, o presente trabalho apresenta a Informática Forense como ferramenta incontornável para combater aquele flagelo. Ao longo da revisão da literatura, evidenciam-se cenários concretos e recorrentes na investigação da criminalidade económica, no sentido de concretizar em fase posterior, o respectivo tratamento com recurso a ferramentas *Open Source*, confrontando os resultados obtidos com os resultantes de idêntico tratamento efectuado com base numa ferramenta comercial de referência.

Procura-se assim demonstrar que estão disponíveis ferramentas que possibilitam um salto qualitativo nos processos de investigação, sem por em causa o equilíbrio orçamental que a actual situação económica exige.

Palavras-Chave:

Informática Forense, Forense Digital, Evidência Digital, Investigação de Crime Económico.

ABSTRACT

In addition to the extraordinary economic development provided by the evolution of Information and Communication Technologies, boosted in recent years, with the development of internet, will be consolidating an anarchic and obscure dimension that, under cover of anonymity and exploiting the same technology, conveys a myriad of behaviors of a criminal nature, which tend to undermine the basic principles of living in society, some of which have contributed greatly to the dimensions of this economic crisis.

Many of the difficulties that the generality of the justice systems faced to master this new type of crime, rooted in the Technological Gap between the means used by organized crime and those that have the justice system.

Taking as reference the phenomenon of economic crime, this dissertation presents the Forensic Computing as a tool essential to combat that scourge.

Through the literature review, I will seek to show, specific scenarios, but recurrent in the investigation of economic crime, in order to realize at a later stage, their treatment with the use of Open Source tools, comparing the results obtained with the same treatment carried out based on a commercial reference tool.

Thus I will show that tools are available that enable a qualitative jump in research processes, without jeopardizing the budget balance of the justice departments, as the current economic situation requires.

Keywords:

Computer Forensics, Digital Forensics, Digital Evidence, Economic Crime Investigation.

Índice

Índice de Figuras:

Índice de Tabelas:

Lista de Abreviaturas:

AFF	—	Advanced Forensic Format
ASCII	—	American Standard Code for Information Interchange
CFTT	—	Computer Forensic Tool Testing
CHS	—	Cylinder-Head-Sector
DCO	—	Device Configuration Overlay
DFRWS	—	Digital Forensic Research Workshop
EWF	—	Expert Witness Format
FAT	—	File Allocation Table File System
FIPS	—	Federal Information Processing Standards
FTK	—	Forensic Tool Kit
HPA	—	Host Protected Area
IOCE	—	International Organization on Computer Evidence
LBA	—	Logic Block Addressing
MBR	—	Master Boot Record
MD5	—	Message-Digest Algorithm
MRU	—	Most Recently Used
NIST	—	National Institute of Standards and Technology
NSRL	—	National Software Reference Library
NTFS	—	New Technology File System
OBEGEF	—	Observatório de Economia e Gestão de Fraude
RDS	—	Reference Data Set
SHA	—	Secure Hash Algorithm
SWGDE	—	Scientific Working Group on Digital Evidence
UNODC	—	United Nations Office on Drugs and Crime
USB	—	Universal Serial Bus

1. INTRODUÇÃO

Para fazer face à multiplicidade de ameaças que se desenvolveram no âmbito da Internet ao ritmo vertiginoso a que esta evoluía, foram-se desenvolvendo ferramentas e técnicas destinadas a detectar e repelir essas ameaças, bem como, a isolar evidências capazes de provar em tribunal este tipo de práticas criminais, as quais, dão hoje corpo a um novo ramo das ciências forenses.

A Informática Forense visa assim combater a criminalidade informática, tendo por base o pressuposto da prática de um crime, sempre que este envolva como meio ou instrumento, o computador ou fazendo do próprio computador o alvo desse acto criminoso.

Um dos efeitos mais significativos da evolução das Tecnologias da Informação e Comunicação, no mundo dos negócios, consiste na crescente desmaterialização dos documentos de suporte. Constata-se actualmente que a maior parte da informação gerada no mundo é criada e armazenada em formato digital e estima-se que mais de metade da documentação relacionada com a actividade económica, nunca deixará o domínio digital. Isto significa que os documentos em formato papel, associados ao mundo dos negócios, constituem apenas uma pequena parte, sendo significativamente maioritário, o número de documentos em formato digital. (Grantz e Reinsel, 2010).

Esta realidade contrasta com o domínio que o papel continua a exercer no campo da justiça onde, com aparente indiferença ao impacto da evolução tecnológica a todos os níveis da sociedade actual, as equipas de investigação, nomeadamente na área do crime económico, continuam a basear o seu trabalho no "*paper discovery*".

A transferência dos suportes documentais para o mundo digital, faz com que os equipamentos informáticos, para além de instrumento e/ou alvo de crimes informáticos, se constituam hoje como imensos repositórios de evidências da prática de crimes da mais variada natureza, nomeadamente económicos, tornando-se hoje incontornável o seu contributo para a descoberta da verdade na generalidade das investigações, independentemente do tipo de crime praticado.

Com a certeza de que a tecnologia pode dar um valioso contributo neste campo, o presente trabalho de investigação, enquadra-se no âmbito da Informática Forense. Nele

se apresenta e avalia um kit de ferramentas de código aberto, capaz de assegurar um conjunto significativo de tarefas no âmbito da investigação de práticas relacionadas com o crime económico.

São evidenciadas as vantagens que o uso das metodologias e ferramentas associadas à "Informática Forense", podem acrescentar ao processo de investigação deste tipo de crimes.

1.1. ENQUADRAMENTO E MOTIVAÇÃO

O crime económico vem assumindo nos últimos anos um protagonismo crescente, quer pela frequência com que é praticado, quer pelos elevados montantes envolvidos, levando-o a atingir uma dimensão cada vez mais relevante e não deixando ninguém imune aos seus efeitos. Do Parlamento Europeu às pequenas empresas; dos bancos aos hospitais; do Estado aos particulares, todos nós, cidadãos comuns, somos potenciais alvos. Apropriação e utilização indevida de recursos, corrupção, fuga ao fisco, transacções visando branqueamento de capitais, manipulação dos registos contabilísticos, utilização de cheques e documentos de identificação falsos, falsificação de cartões de crédito ou débito, venda de bens inexistentes, etc., fazem parte de uma lista infindável de ilegalidades e ilicitudes que a nossa compreensão tem dificuldade em inventariar.

Não se trata, contudo, de um fenómeno recente, como provam os estudos conduzidos por Friedrich Schneider, "New Estimates for the Shadow Economies all over the World" ao fornecer estimativas sobre este fenómeno entre 1999 e 2007, (Schneider et al, 2010).

A generalidade dos crimes económicos tradicionais, têm hoje uma versão "*Cyber*", que oferece mais e melhores oportunidades aos criminosos, proporcionando-lhes maior retorno correndo menores riscos. (NFC, 2010).

Entretanto, a crise económica que actualmente vivemos, evidenciou com o traço dramático das catástrofes, situações de fraude, que se desenvolveram ao longo de anos na sombra de gabinetes de luxo, servindo-se para tal do potencial disponibilizado pelas tecnologias de informação e comunicação, as quais só foram detectadas após o completo esgotamento das reservas de organizações financeiras, até então absolutamente insuspeitas.

Porém, enquanto vemos Bernard Madoff, responsável por uma fraude financeira cometida nos EUA ao longo de cerca de duas décadas, ser efectivamente condenado no final de um processo de investigação concluído em escassos meses[1], habituámo-nos a assistir no nosso país ao desfilar de diversos processos de investigação por práticas semelhantes, arrastando-se penosamente ao longo de vários anos, sem que deles resulte qualquer condenação, acabando frequentemente arquivados por insuficiência de provas, sem que a sociedade se veja ressarcida sequer, dos bens entretanto desviados.

Esta realidade não só degrada a confiança da generalidade da população no sistema de justiça, como reforça o sentimento de impunidade dos criminosos, incentivando-os a multiplicar este tipo de práticas.

Desenvolvimentos tecnológicos como a crescente miniaturização e diversificação de dispositivos capazes de processar e armazenar informação digital, com impacto significativo no aumento exponencial do volume de informação digital armazenado; o alcance planetário da Internet; o surgimento do comércio electrónico; a crescente sofisticação do sector bancário e o novo paradigma do "*Cloud Computing*" baseado no potencial da virtualização que, beneficiando da redução do custo das comunicações e do hardware, proporcionam ambientes complexos, que disponibilizam serviços partilhados por múltiplos organismos dispersos geograficamente à escala global, têm vindo a facilitar de forma significativa a prática de crimes económicos.

Paralelamente, ao nível de sofisticação tecnológica verificado na prática deste tipo de crimes, parece não ter correspondido idêntica evolução nas técnicas utilizadas para o seu combate por parte das autoridades judiciárias.

Com a crescente desmaterialização dos documentos, e o seu armazenamento no formato digital em grandes volumes, nos mais diversos dispositivos, formatos e localizações, o papel da "Informática Forense" como metodologia para recolha e análise de prova digital, revela-se fundamental em praticamente todas as investigações quer judiciais quer corporativas.

Para dar resposta a esta realidade, as autoridades judiciais necessitam, para além de eventuais ajustamentos ao nível da legislação, de recorrer a novos métodos e tecnologias

[1] Timeline: Key dates in the Bernard Madoff case in http://www.guardian.co.uk/business/2009/mar/12/bernard-madoff-timeline-fraud

que permitam isolar, nestes ambientes, evidências digitais capazes de provar em tribunal, a prática de tais crimes.

1.2. ÂMBITO DE INTERVENÇÃO

Não obstante estarem disponíveis no mercado diversas ferramentas vocacionadas para a recolha e análise de evidências digitais, na sua maioria são ferramentas proprietárias com custos de licenciamento de tal modo elevados, que as torna inacessíveis à maior parte dos organismos que delas necessitam, face à exiguidade dos respectivos orçamentos.

A actual conjuntura económica, reclama alternativas e a opção por ferramentas de código aberto, sem custos de licenciamento associados, constitui uma alternativa válida dado que estão disponíveis, não só ferramentas alternativas, como complementares às ferramentas proprietárias que encontramos no mercado.

Acresce que, tal como refere Carrier, (2003), o software de código aberto apresenta neste campo uma vantagem sobre o software proprietário, na medida em que este pode ser examinado e testado por toda a comunidade, enquanto a capacidade de análise do software proprietário é geralmente limitada a um pequeno grupo de programadores que participam no respectivo desenvolvimento no âmbito de uma única empresa, (Carrier, (2003a).

Naturalmente que a fiabilidade deste tipo de ferramentas tem de estar acima de qualquer suspeita, para que os resultados por elas produzidos não sejam postos em causa em fase de julgamento, por parte da autoridade judicial. Esse desiderato esteve na base da criação do projecto Computer Forensic Tool Testing (CFTT), no âmbito do National Institute of Standards and Technology (NIST), com o objectivo de estabelecer uma metodologia para teste de ferramentas de software utilizado em Informática forense, de modo a garantir que os instrumentos utilizados nas investigações de crimes produzem resultados válidos.

1.3. QUESTÃO DE INVESTIGAÇÃO E OBJECTIVO GERAL

A presente dissertação tem como objectivo geral demonstrar a eficácia das ferramentas *open source* no processo de investigação de casos reais de práticas criminais de natureza económica, confrontando os resultados obtidos, com os produzidos pela plataforma comercial de referência “EnCase Enterprise”.

1.4. ABORDAGEM METODOLÓGICA

Durante a realização desta dissertação, foram desenvolvidas quatro fases metodológicas fundamentais:

1. Revisão da Literatura;
2. Levantamento de hipóteses;
3. Recolha e análise de dados referenciados a cenários de crime económico;
4. Análise de resultados para validação das hipóteses.

A primeira fase, consiste na revisão da literatura relacionada com o fenómeno do crime económico, evolui para idêntica tarefa no campo da Informática Forense, pondo a ênfase em questões relacionadas com o crime económico.

Seguiu-se a identificação de cinco hipóteses de investigação, resultantes da anterior fase de revisão de literatura sobre informática forense. As hipóteses formuladas têm por base desafios e cenários representativos no contexto da investigação de crimes económicos.

Numa terceira fase, primeira do trabalho empírico, são montados os cenários representativos de investigação de crime económico, com o objectivo de proceder à realização de testes em contexto laboratorial (segunda fase do trabalho empírico) seguida de recolha de dados para cada caso (terceira fase do trabalho empírico). Nesta fase foram utilizadas ferramentas proprietárias de referência, bem como as ferramentas *open source* mais ajustadas aos cenários em análise.

Na quarta e última fase metodológica, são analisados os resultados dos testes para cada caso de crime económico através de uma análise comparativa de resultados obtidos e produzidos pelas diferentes ferramentas, validando assim a maioria das hipóteses de investigação

Finalmente são apresentadas as conclusões globais sobre a possibilidade de utilização de ferramentas *open source* no desempenho e desenvolvimento das várias fases do trabalho forense digital, relacionado com o crime económico.

1.5. ESTRUTURA DA DISSERTAÇÃO

O presente trabalho de investigação está estruturado em duas partes, em função da natureza dos capítulos de cada uma delas.

A primeira parte engloba cinco capítulos de carácter essencialmente teórico, o primeiro dos quais assegura o enquadramento do trabalho de investigação, ocupando-se os restantes da revisão da literatura que começa por caracterizar a problemática do crime económico no capítulo 2. O capítulo 3 desenvolve a temática da informática forense, seus fundamentos, metodologias e ferramentas. Prossegue no capítulo 4 com a problemática da recolha de prova, visando clarificar o papel da Informática forense no combate ao crime económico bem como evidenciar quais as condicionantes para o seu aproveitamento pleno, por parte da autoridade judicial. O capítulo 5 conclui a fundamentação teórica estabelecendo algumas regras quanto à plataforma de análise a utilizar na componente empírica da dissertação.

A segunda parte, de natureza prática, dedicada à investigação empírica, compreende o Capítulo 6, no qual são apresentadas ferramentas e métodos de tratamento adequados para dar resposta aos cinco cenários identificados ao longo da revisão da literatura, interpretados os resultados obtidos tendo por objectivo validar as hipóteses associadas aos referidos cenários.

Por último, o capítulo 7 tratará das considerações finais da investigação, sob a forma de conclusões apontando ainda as limitações do presente estudo, bem como, sugestões para futuras investigações.

2. CRIME ECONÓMICO

Neste capítulo faz-se uma abordagem à problemática do crime económico, realçando o seu carácter universal, evidenciando o papel que as novas tecnologias de informação e comunicação desempenham no recente crescimento exponencial deste tipo de criminalidade. Paralelamente, aponta-se o recurso às mesmas tecnologias como forma privilegiada de prevenir e combater este tipo de práticas.

2.1. DEFINIÇÃO E AMPLITUDE DO CRIME ECONÓMICO E FINANCEIRO

As práticas de corrupção, bem como todas as práticas associadas ao crime económico e financeiro, são encaradas como actos de natureza desviante e criminosa pois, para além de violarem as regras estabelecidas para o funcionamento das instituições no seu todo, contribuem para suscitar nos cidadãos sentimentos generalizados de desconfiança social, podendo, no limite, se nada for feito para o contrariar, degenerar num processo vertiginoso de decadência das mais elementares regras da sã vivência social, cultural, económica e política (Jain, 2001).

Entende-se por "crime económico e financeiro", toda a forma de crime não violento que tem como consequência uma perda financeira e como objectivo um ganho financeiro ilegítimo. Este tipo de crime, engloba assim uma vasta gama de actividades ilegais, como a corrupção, a fraude, a evasão fiscal e o branqueamento de capitais, entre outros.

É, no entanto, difícil definir o conceito de "crime económico", e fazê-lo com exactidão continua a ser um desafio. A tarefa complicou-se ainda mais devido aos avanços tecnológicos, que proporcionam novos meios para desenvolver e perpetuar crimes desta natureza (UNODC, 2005).

É igualmente difícil determinar a amplitude global do fenómeno, em parte devido à ausência de um conceito claro e aceite por todos, em virtude dos sistemas de registo do crime económico e financeiro diferirem consideravelmente de país para país, bem como, pelo facto das empresas ou instituições financeiras optarem por resolver os incidentes internamente, abstendo-se de os participar às autoridades (Pimenta, 2009).

Não obstante esta dificuldade, enraíza-se cada vez mais na sociedade moderna, a noção de que o crime económico e financeiro, nomeadamente a fraude, é o tipo de crime que apresenta mais rápido crescimento.

2.2. O IMPACTO DOS AVANÇOS TECNOLÓGICOS

Os consideráveis avanços na tecnologia transformaram profundamente, quer os fluxos mundiais de informação, quer o modo de negociar. O alcance planetário da Internet; o surgimento do comércio electrónico; a crescente sofisticação do sector bancário, a par de muitas outras evoluções tecnológicas; deram lugar ao aparecimento de grupos criminosos com formas de organização cada vez mais sofisticadas. A utilização fraudulenta de cartões de crédito ou débito, tornou-se um negócio à escala global. A fraude de identidade, envolvendo a recolha de dados pessoais de indivíduos e a subsequente falsificação da respectiva identidade constitui uma outra actividade criminosa com elevado crescimento, que tem implicações directas no fenómeno do "Crime Económico".

Por outro lado, a maior parte dos crimes de natureza económica, praticados com base na tecnologia, não exigem a presença física do infractor. A existência de diferenças significativas entre os quadros jurídicos dos diversos países, permite que os criminosos possam escolher, para base da sua actividade, países com quadros jurídicos mais brandos.

Os dados disponíveis sugerem inequivocamente, que o crime económico e financeiro continua a crescer rapidamente (PwC, 2009), impulsionado pelo efeito das novas tecnologias de informação, da generalização das operações bancárias por via electrónica e da expansão dos serviços da Internet à escala global.

2.3. O IMPACTO NO DESENVOLVIMENTO SUSTENTÁVEL

Tendencialmente, as actividades fraudulentas ocupam o lugar das actividades económicas legítimas, desincentivando o investimento. Daí que, os crimes económicos e financeiros constituam, a longo prazo, uma ameaça grave ao desenvolvimento sócio-económico pacífico e democrático. Os países onde as actividades económicas e financeiras ilegais são socialmente aceites, não oferecem condições para que os mercados financeiros se desenvolvam, dados os elevados critérios e valores profissionais, jurídicos e morais em que estes assentam. A mera noção de que estão a ser cometidos actos económicos e financeiros ilegais, pode causar danos económicos irreparáveis. A suspeita pública mina inexoravelmente a legitimidade do governo (Branco, 2010).

Revela-se crucial fazer face a esta forma de crime, na perspectiva do desenvolvimento sustentável e do reforço das capacidades.

2.4. PREVENIR E CONTROLAR OS CRIMES ECONÓMICOS E FINANCEIROS

É necessária uma acção mais eficaz da parte da comunidade e das instituições internacionais no combate ao crime económico e financeiro. No âmbito das Nações Unidas, o Grupo de Alto Nível sobre Ameaças, Desafios e Mudança, identificou o crime organizado transnacional como uma grave ameaça para a comunidade internacional e recomendou que fosse negociada uma Convenção Internacional Global sobre o Branqueamento de Capitais. Ainda que nenhum instrumento internacional trate especificamente o problema do crime económico e financeiro, tanto a Convenção das Nações Unidas contra o Crime Organizado Transnacional como a Convenção das Nações Unidas contra a Corrupção contêm disposições que permitem estabelecer uma estrutura internacional para responder às actividades criminosas deste tipo.

Uma abordagem global comum deste problema, poderá contribuir para reforçar ainda mais os mecanismos internacionais de aplicação da lei e de cooperação. É, contudo, indispensável atingir a normalização de definições jurídicas dos crimes económicos e financeiros, bem como assegurar a criação das competências necessárias para a investigação destes actos nos serviços de repressão e aplicação da lei, em particular nos países em desenvolvimento. O Gabinete das Nações Unidas contra a Droga e a Criminalidade já presta assistência técnica, com vista a ajudar os Governos a reforçarem as suas capacidades de luta contra o crime económico e financeiro, em particular no que respeita ao branqueamento de capitais (UNODC, 2005).

O carácter universal deste fenómeno é uma realidade incontornável. Jain, (2001), refere que os efeitos da corrupção tendem a repercutir-se por toda a economia, não se confinando ao acto específico. Constatou ainda que, num país com um sistema legal ineficaz o nível de corrupção tende a crescer podendo levar a que a respectiva elite política não consiga resistir ao aumento do rendimento que esta proporciona. Uma vez corrompida, essa elite tentará reduzir a eficácia dos sistemas legal e jurídico, através da manipulação da atribuição de recursos e nomeações para cargos-chave. Por sua vez, a redução dos recursos, vai condicionar o combate permitindo assim que a corrupção se dissemine ainda mais (Jain, 2001).

A recente crise económica fez multiplicar as vozes que reclamam a necessidade urgente de investigar e punir os culpados, ao ponto de, eminentes especialistas, defenderem que a magnitude de alguns dos crimes praticados deveria levar ao seu enquadramento como "Crimes contra a Humanidade", como se pode constatar no artigo publicado na Businessweek, em Março de 2009 (Zuboff, 2009).

2.5. PANORAMA INTERNACIONAL

A dinâmica do capitalismo assenta nas empresas privadas e na sua capacidade de gerar dividendos. A crescente mundialização e unificação dos mercados aumenta a pressão para que se potencie o lucro. Estamos perante uma situação intrínseca ao funcionamento da nossa própria sociedade. Contudo, é essa mesma situação, que pode levar as empresas a apostarem no curto prazo e esquecerem o longo prazo, a introduzir informações nos documentos contabilísticos que não correspondem ao valor criado, transmitindo uma leitura deturpada quer para a sociedade quer para muitos dos seus stakeholders. Inevitavelmente, estes comportamentos estão associados a ganhos de uns e perdas de outros (Pimenta, 2009).

Muitas fraudes são de uma simplicidade impressionante, o que as torna praticáveis e despercebidas, jogando frequentemente com a ignorância generalizada e a ânsia de lucro fácil que é apanágio da natureza humana. Mas muitas outras, são altamente sofisticadas, de difícil compreensão e detecção, estudadas por cérebros brilhantes legalmente contratados em exclusivo para esse efeito.

Frequentemente as fronteiras entre o que é "normal" e o que é fraudulento são muito difusas e difíceis de estabelecer, mesmo quando estamos perante práticas que são reconhecidamente intencionais.

Não é preciso recuar muito no tempo para constatar que os fraudulentos de hoje foram os exemplos a seguir na véspera. O exemplo da crise da Islândia é testemunho claro desta incongruente histeria e a actual crise económica é, sem sombra de dúvida, consequência de práticas criminais desta natureza.

Na décima oitava sessão da Comissão sobre Prevenção do Crime e Justiça Criminal, o Director Executivo do United Nations Office on Drugs and Crime [UNODC], proferiu a seguinte afirmação: "*...os banqueiros têm permitido que o Crime Económico se torne parte da economia global*" (UNODC, (2009)).

E acrescentou:

> *"a crise financeira está a proporcionar uma oportunidade extraordinária para a penetração da máfia pois, face à asfixia que se abateu sobre as instituições financeiras, as organizações criminosas apresentam-se hoje, como uma das poucas fontes de crédito..."*

Enron, WorldCom, Lehman brothers, Bernard Madoff, retratam evidências que todos pudemos constatar recentemente, através das notícias veiculadas pela generalidade dos órgãos de comunicação social.

2.6. PANORAMA NACIONAL

Estudos conduzidos pelo Observatório de Economia e Gestão de Fraude (OBEGEF), revelam ser possível estimar que, no nosso País, o fenómeno da fraude representa entre 1,5% e 2,0% do PIB nacional e a fraude ocupacional 10% do volume de vendas (Pimenta, 2009). Por outro lado, o volume da economia informal ronda os 23% (Afonso e Gonçalves, 2009). A estes dados acrescem diversos casos mediatizados como os casos BPN e BPP na banca, e diversos outros envolvendo altas individualidades que ocuparam cargos governativos de relevo, todos em fase de investigação.

2.7. A EVOLUÇÃO DO SUPORTE DOCUMENTAL

As vantagens inerentes aos documentos electrónicos desencadearam um progressivo e generalizado processo de desmaterialização que, com maior ou menor rapidez, se disseminou por grande parte das áreas de actividade. O desenvolvimento do comércio electrónico ajudou a sedimentar essa tendência ao ponto de se estimar que apenas 5% dos novos documentos, sejam criados fora do mundo digital e que, apenas uma ínfima parte dos documentos digitais, chegará a ser impressa.

Entre nós, o Livro Verde para a Sociedade da Informação (1997), apontava já a necessidade de se viabilizar e dinamizar o comércio electrónico e a transferência electrónica de dados, incluindo a sua promoção na Administração Pública. Seguiu-se a aprovação do documento orientador para a Iniciativa Nacional do Comércio Electrónico, no âmbito do qual é enunciado o objectivo de promoção do uso de meios de comércio electrónico pela Administração Pública e de preparação de legislação para o reconhecimento jurídico da factura electrónica, que veio a ser publicada em Diário da República.

2.8. O PROCESSO DE INVESTIGAÇÃO

Por norma, a abertura de um inquérito para investigação de práticas ilícitas de natureza económica tem por base uma denúncia ou uma acção de inspecção administrativa. Este facto leva a que se verifique um intervalo de tempo significativo, entre o início da investigação e a data em que os factos ocorreram.

Neste contexto, o processo de investigação de um crime de natureza económica tem, normalmente, um carácter retrospectivo, assentando essencialmente na recolha de documentação que permita provar os indícios da sua prática efectiva.

Tradicionalmente, essa recolha visava documentação em suporte papel que, ainda hoje, continua a ser o suporte comummente aceite pelas autoridades judiciárias, tal como referem Galves e Galves, (2004), em artigo publicado no Criminal Justice Magazine:

> "*Infelizmente, é ainda raro o reconhecimento pleno, por parte dos agentes da justiça, do potencial tecnológico da evidência digital para ajudar a resolver crimes e processar criminosos. …tradicionalmente a prática da aplicação da lei tende a dar maior relevo às provas físicas focando-se mais na recolha e inspecção de evidência não-tecnológica*." (Galves e Galves, 2004).

Contudo, face à evolução tecnológica verificada, é inevitável que a recolha de prova digital passe a assumir um papel preponderante neste tipo de investigações.

Tendo em conta que os suportes informáticos examinados durante uma investigação, poderão, em algum momento, servir de prova legal num tribunal civil ou criminal, a forma como os dados são recolhidos, autenticados e analisados torna-se extremamente crítica.

Em situações dessa natureza, o recurso às metodologias da Informática Forense, que visam determinar a dinâmica, a materialidade e a autoria de ilícitos, através da identificação, processamento e transformação de evidências digitais em provas materiais do crime, recorrendo a métodos técnico-científicos, com a finalidade de lhes conferir validade probatória em juízo, mostra-se indispensável.

Trata-se de um processo que se desenvolve em dois domínios:

- Domínio puramente investigatório, de carácter técnico-informático que envolve as tarefas de preservação, localização, selecção e validação das evidências;

- Domínio legal, de carácter técnico-jurídico, que envolve a construção da argumentação no sentido de assegurar a reconstrução dos factos investigados.

A figura 1 retrata o conjunto das etapas sequenciais que integram cada um dos domínios.

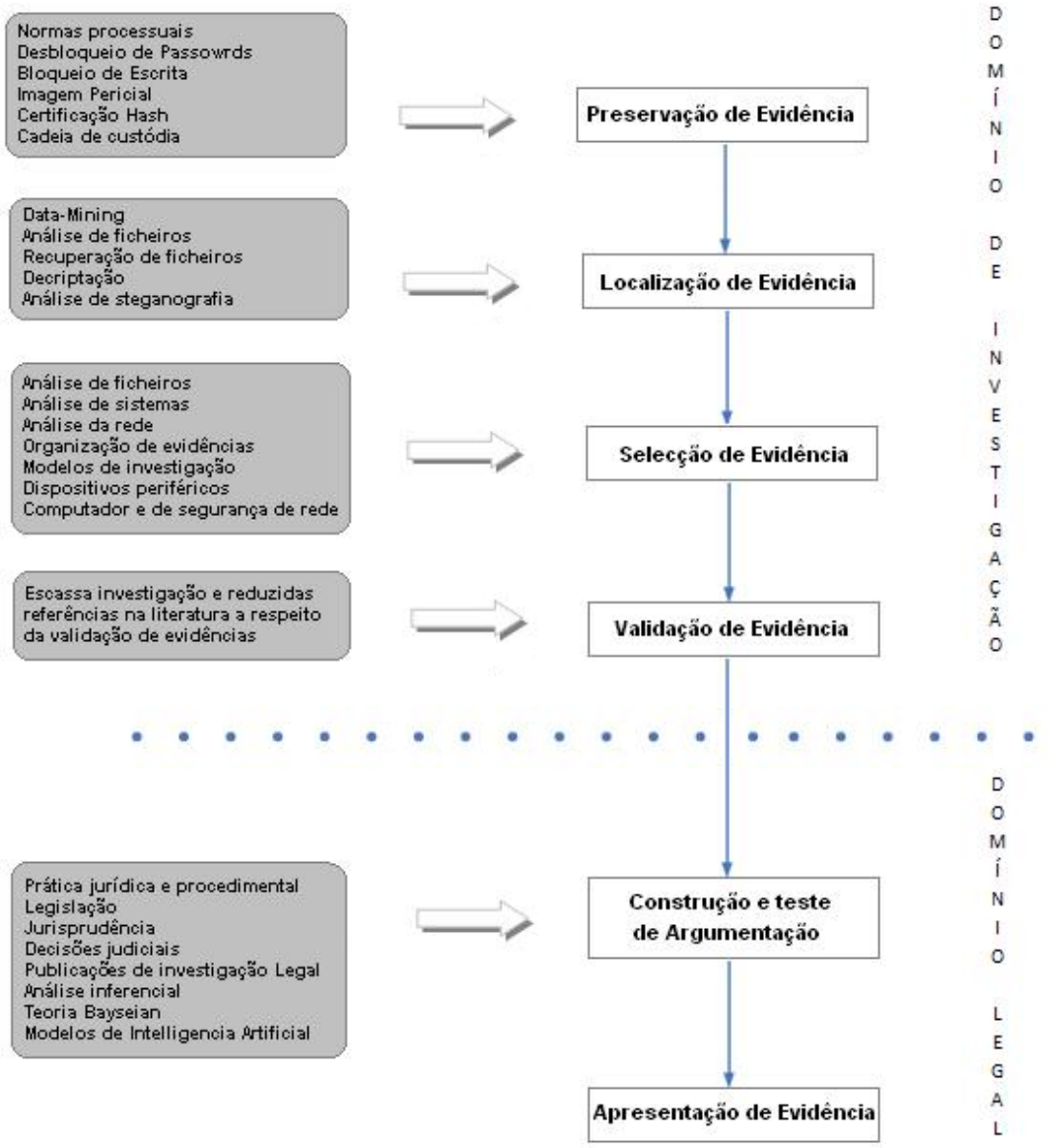

Figura 1. *Etapas do processo de investigação (adaptado de Boddington, Hobbs & Mann, 2008).*

3. INFORMÁTICA FORENSE

Este capítulo tem por objectivo enquadrar a Informática Forense como ramo das ciências forenses e apresentar o respectivo "Estado da Arte", abordando o conceito de evidência digital, principais fontes onde podemos encontrar este tipo de amostras, metodologias, técnicas e ferramentas base mais utilizadas.

3.1. INTRODUÇÃO

O mundo, cada vez mais complexo, em que vivemos coloca-nos numa encruzilhada social e cultural muito particular. Em nenhum outro momento a sociedade foi tão dependente da tecnologia nas suas mais diversas expressões. Quase todas as facetas da nossa vida sofrem, de alguma forma, o impacto da tecnologia (e-mail, instant messaging, Internet banking, vídeo e música digital, etc.). Esta dependência bem como a dependência da tecnologia na sua globalidade, teve um efeito em cascata sobre outras áreas menos óbvias da sociedade, como retrata de forma eloquente Bruse Schneier, no seu livro Secrets and Lies-Digital Security in a Networked World (Schneier, 2004).

Uma dessas áreas é a aplicação da lei e, mais especificamente, na parte que diz respeito à investigação criminal (Kruse e Heiser, 2001). Historicamente, a investigação criminal contou com conceitos tais como: evidência física, testemunhas oculares, e confissões. Hoje, o investigador criminal não pode deixar de reconhecer que uma parte significativa da prova, reside na forma electrónica ou digital. Conforme refere Carrier, (2002) no seu artigo Getting physical with Digital Investigation Process, para muitos crimes da actualidade, a cena do crime pode consistir num simples computador que, por si só, pode comportar um elevado número de evidências, em oposição à tradicional cena de crime "físico". A testemunha de hoje, pode ser amanhã um ficheiro de 'log' gerado num computador.

Para que se possa lidar eficazmente com esta nova realidade, a informática forense, enquanto ramo embrionário da ciência, vem desenvolvendo regras e criando metodologias no sentido de alertar para os cuidados que devem ser tomados para assegurar que não é descurado o objectivo primordial do processo de investigação, o qual, em última instância, visa identificar a parte ou partes responsáveis pelas práticas ilegais.

3.2. A CIÊNCIA FORENSE

Tal como a medicina ou a engenharia, a análise forense de evidências físicas é uma ciência aplicada, que assenta sobre os princípios científicos básicos da física, química e biologia. Como tal, cada experiência e cada caso, deve seguir o método científico de teste de hipóteses.

Não obstante as conclusões a que chegaram Inmon e Rudin, (2001) no seu trabalho "Principles and Practice of Criminalistics", referindo que a prática forense não é de natureza estritamente experimental, dada a natureza completamente descontrolada da amostra que caracteriza os processos de investigação, por contraponto às condições extremamente controladas, em que se realizam as experiências científicas com variáveis intencionalmente alteradas, uma de cada vez. O método científico tem sido uma das mais poderosas ferramentas disponíveis para assegurar ao investigador forense o cumprimento da sua responsabilidade de fornecer provas precisas relevantes de forma objectiva e imparcial.

Partindo da recolha de factos, prossegue com a formulação de uma hipótese com base nas provas disponíveis, mantendo, no entanto, consciência da possibilidade de que as observações ou análises efectuadas, possam não estar correctas. Assim, para avaliar a veracidade da hipótese formulada, é não só necessário procurar suporte para as provas encontradas mas igualmente importante considerar hipóteses alternativas. O processo de tentar refutar a nossa própria hipótese envolve a realização de experimentações que permitam testar as nossas suposições subjacentes e obter uma melhor compreensão dos vestígios digitais que estamos a analisar.

Trata-se de um processo inerentemente indutivo em que, os resultados obtidos a partir de uma amostra forense, não são uma simples experiência, mas um exame ou análise no qual, o analista recolhe factos sobre um pedaço de evidência que, mais tarde, vai combinar com outros factos e hipóteses, de modo a formar uma teoria sobre o que efectivamente aconteceu, no caso em análise.

3.3. A CIÊNCIA FORENSE NO CAMPO DIGITAL

No que respeita à Informática Forense, alguns autores consideram que esta combina as vantagens da ciência forense, com a arte da investigação. Venema e Farmer no seu livro Forensic Discovery, referem que, algumas vezes o perito actua como arqueólogo (digital), outras como geólogo (digital) (Farmer e Vanema, 2005).

Arqueólogo digital, quando actua sobre os efeitos directos da actividade do utilizador, como o conteúdo do ficheiro, tempos de acesso, informação sobre ficheiros apagados e informação sobre o tráfego de rede;

Geólogo Digital, quando actua sobre os processos autónomos do sistema, sobre os quais o utilizador não tem controlo directo, como a atribuição e reciclagem de blocos de disco, números de identificação de ficheiros, páginas de memória ou números de identificação de processos.

Como exemplo, os autores fazem notar que os utilizadores têm controlo directo sobre o conteúdo dos ficheiros existentes (arqueologia). Porém, quando um ficheiro é apagado, os utilizadores deixam de ter qualquer controlo sobre a sequência de destruição operada pelo sistema (geologia).

Na mesma linha, Carrier, (2006) reflecte sobre a forma como deve ser designada esta actividade, comparando-a com a análise forense comum. Na sua opinião, contrariamente à análise forense comum (física), em que o especialista é confrontado com um conjunto limitado de questões sobre amostras (fluidos, balas, amostras de pele, cabelo, etc.), que lhe são entregues por um detective, cabendo-lhe tarefas de identificação e individualização, a Informática forense abarca o papel do próprio detective, desenvolvendo a sua acção em duas etapas: busca de provas, seguida da respectiva análise e interpretação. Nessa medida, este autor propõe para esta actividade, a designação "Computer Forensic Investigation" ou "Digital Forensic Investigation".

Figura 2 *- Núcleo de Investigação de Computação Forense Adaptado de Palmer, (2001)*

3.4. INFORMÁTICA FORENSE: DEFINIÇÃO

O relatório técnico do primeiro "Digital Forensic Research Workshop (DFRWS)" define "Informática Forense" como o ramo das ciências forenses que, recorrendo a ferramentas e metodologias cientificamente comprovadas, assegura a identificação, preservação, recolha, validação, análise, interpretação, documentação e apresentação de evidências digitais, recolhidas a partir de qualquer dispositivo que armazene ou processe informação no formato digital, com o objectivo de facilitar ou favorecer a reconstrução de eventos relacionados com práticas criminalizáveis (Palmer, 2001).

A Informática Forense revela-se assim uma área com um extenso âmbito, mas em constante desenvolvimento, exigindo o recurso a um número significativo de diferentes ferramentas destinadas a executar funções específicas muito variadas.

No que respeita às ferramentas disponíveis, também aqui, tal como noutros ramos da informática, se esgrimem argumentos entre código aberto e código fechado, quer sejam de natureza meramente filosófica (Stallman, 2011), quer relacionadas com questões de suporte e fiabilidade (Prasad, 2001), quer ainda quando à segurança (Wheeler, 2003). Naturalmente que, cada um destes campos arregimenta grupos de utilizadores em redor da respectiva argumentação, sem contudo se vislumbrar um claro vencedor.

No caso concreto da Informática Forense, estas ferramentas são utilizadas para analisar informação digital, com o objectivo de encontrar elementos que permitam provar que alguém praticou ou deixou de praticar um dado crime, provas essas que serão posteriormente apreciadas num tribunal, podendo persuadir os jurados a restringir ou mesmo eliminar as liberdades individuais.

Tradicionalmente, os tribunais têm provado constituir excelentes campos de teste para a pesquisa científica séria (Palmer, 2001) e, tendo em conta as especificidades legalistas que caracterizam este tipo de prova, (Carrier, 2002) argumenta que as ferramentas de código aberto, reúnem condições para satisfazer de uma forma mais clara e abrangente, os requisitos legais estabelecidos, do que as ferramentas de código fechado.

3.5. EVIDÊNCIA DIGITAL

Ao "mundo" físico que nos rodeia, caracterizado por uma natureza determinística e finita, no qual, propriedades intangíveis tais como o tempo, o espaço, a identidade ou a localização física surgem como inalteráveis, encontrando-se qualquer delas fora do nosso controlo, contrapõe-se um "mundo" digital onde as acções são virtualmente

independentes quer do tempo quer da localização física e no qual, com adequados conhecimentos, é possível alterar cada uma das propriedades antes referidas.

Por outro lado, no "mundo" físico, o investigador pode observar directamente muitos estados e eventos, usando os seus próprios sentidos, enquanto, no "mundo" digital, essa observação é indirecta pois só com recurso a hardware e software adequados, é possível observar eventos e estados digitais.

Esta realidade tem um impacto muito significativo no campo da Informática Forense, dado que, frequentemente, conseguimos provar com facilidade algo no "mundo" físico, que nos levanta grandes dificuldades em imputar a alguém, no "mundo" digital.

A regra fundamental seguida pela ciência forense é o princípio da troca de Locard, segundo o qual "todo o contacto deixa vestígios". Ninguém pode agir (cometer um crime) com a força (intensidade) que o acto criminoso requer, sem deixar para trás inúmeros sinais (vestígios), quer deixando-os no local do crime quer levando-os consigo, sinais esses capazes de denunciar onde esteve e o que fez, (Inman e Rudin, 2001).

Com base na definição de evidência digital por parte de três organizações de referência nesta matéria:

- "*Information stored or transmitted in binary form that may be relied upon in court*" (IOCE, 2002);
- *"Information of probative value that is stored or transmitted in binary form"* (SWGDE, 2009);
- *"Information and data of investigative value that is stored on or transmitted by a computer"* (ACPO, 2011).

diremos que, Evidência Digital, é qualquer informação armazenada ou transmitida em formato digital, com valor probatório em processo judicial civil ou criminal. Também aqui, o princípio da troca de Locard é válido (Carrey, 2009), graças à malha de controlo que os sistemas operativos hoje disponibilizam, possibilitando o rastreio de toda a actividade desenvolvida sobre os sistemas.

Nesse sentido, um princípio básico que não pode ser descurado, consiste na preservação de todos os vestígios originais, o que aconselha a que a investigação não decorra sobre o

suporte original mas, sempre que possível, se procure trabalhar sobre uma cópia integral e exacta desse suporte.

Joseph Rynearson, (2002) refere que qualquer coisa é evidência de algum evento. A chave está em identificar e isolar evidências relacionadas com o incidente em questão. Cada pedaço de dados pode ser usado para suportar ou refutar alguma hipótese, pois a investigação visa isolar os dados relacionados com o crime praticado.

3.6. PRESERVAÇÃO DA EVIDÊNCIA DIGITAL

O facto da informação em formato digital, ser mais facilmente adulterada e/ou forjada do que os materiais físicos, obriga a garantir um alto nível de integridade dos vestígios encontrados em todos os exames periciais. Com o desenrolar dos exames e a descoberta de evidências no material examinado, é fundamental manter a rastreabilidade dessas descobertas e respectivas correlações.

Um aspecto fundamental a ter em conta na preservação de evidências digitais, consiste no estabelecimento e manutenção da respectiva cadeia de custódia, que passa por assegurar um registo sistemático de todo o processo de tratamento, desde a identificação da evidência até à respectiva apresentação em tribunal. (Kruse e Heiser, 2002).

A expressão “Cadeia de Custódia” é um termo jurídico que se refere à capacidade de garantir a identidade e integridade de uma amostra no decurso da sua obtenção durante a sua análise e até ao final do processo. Na prática, consiste em salvaguardar a amostra de forma documentada, de modo que, não se possa alegar que foi modificada ou alterada durante o processo de investigação (Giannelli, 1996).

Quando a prova é constituída por objectos físicos, a prática é armazená-los em sacos ou envelopes selados, com um formulário que identifica quem a recolheu e cada uma das pessoas que entretanto a tenha usado para algo, evitando assim dúvidas sobre quem e quando lhe acedeu.

Com a prova electrónica (imagens de discos e memória, ficheiros de dados e executáveis, entre outros.), a prática consiste em obter assinaturas digitais do respectivo conteúdo, “hash”, no momento da sua recolha, através das quais se possa comprovar em qualquer momento subsequente, que essa prova mantém a respectiva integridade, refutando assim qualquer suspeita sobre eventuais modificações.

Uma cadeia de custódia bem documentada, reforça as garantias de admissibilidade das evidências em tribunal.

Note-se que, as evidências não existem por si só, como algo absoluto, trata-se sim, de material que é usado para estabelecer a verdade de um facto particular, ou estado de coisas. É nessa perspectiva que é entendida pelo tribunal. Por outro lado, a evidência digital não é uma realidade virtual. Na sua essência, ela é composta por campos magnéticos, campos eléctricos e pulsos electrónicos, (Casey, 2000), pelo que, tem tudo para que se possa considerar um tipo de evidência física, embora menos tangível. A diferença, reside no facto de exigir técnicas e ferramentas apropriadas, para a respectiva recolha, análise e apresentação, num formato que possa ser entendido pela generalidade dos intervenientes.

3.7. CARACTERÍSTICAS DA EVIDÊNCIA DIGITAL

A evidência digital possui características muito particulares, que a diferenciam das demais, nomeadamente:(Wang, 2007)

- Pode ser duplicada com exactidão, permitindo a preservação da evidência original durante a análise;
- Com métodos apropriados, é relativamente fácil determinar se uma evidência digital foi modificada;
- A evidência digital é extremamente volátil, podendo ser facilmente adulterada durante o processo de análise;
- É difícil de extinguir, pois mesmo apagando um ficheiro ou formatando um disco rígido, ainda é possível recuperar a informação que este continha;
- É difícil de entender no seu estado puro. Trata-se de campos magnéticos, campos eléctricos e pulsos electrónicos, que necessitam de técnicas e ferramentas apropriadas, para que possam ser recolhidos e analisados.

3.8. METODOLOGIA E LINHAS DE ORIENTAÇÃO

Desde o primeiro Digital Forensic Research Workshop (DFRWS) realizado nos EUA em 2001, na cidade de Utica, que a definição de uma metodologia formal para a análise forense digital, se assume como uma preocupação permanente. Segundo Palmer, (2001) este Workshop reuniu mais de 50 investigadores, especialistas em exames e análises periciais de computadores, oriundos de diversas universidades, e teve por objectivo

primordial o estabelecimento de uma comunidade de pesquisa que aplicasse métodos científicos na busca de soluções, cujos resultados beneficiariam todos os envolvidos na área da Computação Forense. No âmbito desse workshop, foram constituídos diversos grupos de trabalho, o primeiro dos quais com a missão de construir uma taxonomia para orientação da pesquisa e identificação das áreas ou categorias que definem o "universo" da Ciência Forense Digital. O debate gerado, produziu a seguinte definição:

> "*Computação Forense: Consiste na utilização de métodos cientificamente comprovados e derivados para a preservação, recolha, validação, identificação, análise, interpretação, documentação e apresentação de evidências provenientes de fontes digitais com a finalidade de facilitar ou promover a reconstrução de eventos associados a práticas criminalizáveis, ou que ajudem a antecipar acções não autorizadas, que se mostrem prejudiciais a operações planeadas*" (Palmer, 2001).

Esta definição encerra ela própria um procedimento sequencial que, de forma geral, continua a reger as acções de investigação nesta área. Em 2004, o Departamento de Justiça dos EUA (DOJ) divulgou uma brochura intitulada "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", a qual define três orientações base, a observar por quem exerce funções nesta área (Hart, 2004):

- As acções desenvolvidas para proteger e recolher evidências digitais não deverão afectar a integridade dessas evidências;
- Os técnicos envolvidos no exame de evidências digitais devem obter previamente a formação adequada para esse fim;
- As actividades desenvolvidas relativamente à apreensão, análise, armazenamento ou transferência de evidências digitais, devem ser devidamente documentadas, preservadas, e mantidas disponíveis para consulta, de modo que uma terceira parte independente, seguindo os mesmos procedimentos, seja capaz de atingir o mesmo resultado.

Em 1998 foi criado o Scientific Working Group on Digital Evidence (SWGDE) que reúne organizações activamente envolvidas no campo da prova digital e multimédia, para fomentar a comunicação e cooperação, bem como, garantir a qualidade e consistência no seio da comunidade. No âmbito desse organismo, foi constituído um Comité Forense com a missão de promover o uso de técnicas com eficácia

cientificamente comprovada, para a recolha e análise de evidências digitais e multimédia. No mesmo ano, constituiu-se igualmente a International Organization on Computer Evidence (IOCE), com a missão de preparar os princípios internacionais para os procedimentos de recolha de provas digitais, no sentido de garantir a harmonização dos métodos e práticas entre as nações e garantir a capacidade de usar evidências digitais recolhidas por um Estado num tribunal de outro Estado. Destes dois organismos emanaram os seguintes princípios (IOCE, 2002)

- As acções desenvolvidas durante a investigação forense não devem alterar as evidências;
- Toda a evidência recolhida deve ser preservada em local de acesso controlado e livre de alterações;
- Devem ser produzidas cópias das evidências originais e, sempre que possível, a investigação deve ser conduzida sobre essas cópias;
- Tais cópias, devem ser idênticas às evidências originais, contendo toda a informação no seu estado original;
- O investigador não deve confiar cegamente no sistema alvo nem nos programas e bibliotecas dinâmicas nele encontrados;
- Todas as evidências digitais recolhidas, e as cópias produzidas, devem ser autenticadas por meio de assinaturas criptográficas, permitindo a verificação posterior da sua integridade;
- Toda a evidência recolhida deve ser identificada contendo o número do caso em investigação, uma breve descrição da evidência e a data e hora da recolha;
- Todas as informações relativas à investigação, devem ser documentadas de maneira permanente e devem estar disponíveis para revisão;
- Deve ser mantida a cadeia de custódia das evidências recolhidas, documentando o circuito completo de cada evidência durante a investigação. Devem ser registadas, entre outras informações, o nome da pessoa que recolheu a evidência, como, quando e onde foi feita a recolha, o nome do investigador que está de posse da evidência, data e horário de retirada e devolução da evidência e as actividades executadas por cada um dos intervenientes;

- As ferramentas usadas na investigação (hardware e software) devem ser amplamente aceites na área e testadas para garantir a sua correcta operação e fiabilidade;
- O investigador deve ser responsável pelos resultados da investigação e pelas evidências enquanto estiverem na sua posse.

3.9. PROCESSO DE ANÁLISE

No processo de análise, toda a informação relevante deve ser recolhida através de um varrimento meticuloso do dispositivo para posterior análise, respeitando dois princípios básicos: o da autenticidade, segundo o qual deve ser garantida a origem dos dados, e o da fiabilidade, que assegura que os dados são fiáveis e livres de erros (Ghosh, 2004).

O tipo de dados envolvidos no incidente que está a ser investigado, também é importante. Numa situação em que o sistema alvo esteja ligado, é possível a recolha de dados voláteis, como processos em execução, tráfego de rede, conexões abertas, memória do computador e periféricos (impressão e vídeo), entre outros; observando-se a ordem de volatilidade de cada evidência (Farmer e Venema, 2005).

Entretanto, caso o sistema esteja desligado apenas estarão disponíveis os dados não voláteis. Nesse caso, torna-se necessário fazer uma "imagem" do dispositivo de armazenamento, preservando o dispositivo original. No contexto da informática forense o termo "imagem" de um dispositivo de armazenamento, corresponde ao resultado de um processo que envolve a cópia exacta dos dados contidos neste disco (bit a bit), preservando a respectiva estrutura e localização (Brown, 2006).

No processo de aquisição (realização da "imagem"), o dispositivo alvo, presumivelmente envolvido na prática do crime sob investigação, deve ser encarado como qualquer cena de crime que necessita de ser preservada em toda a sua extensão. Tal como as impressões digitais e o DNA, as evidências digitais são igualmente frágeis e podem ser danificadas ou mesmo perdidas se não forem tomadas as devidas precauções. A identificação exaustiva do dispositivo, o local onde se encontrava, o tipo de periféricos a que estava ligado, eventuais ligações a redes LAN's ou WAN's, etc., são elementos que poderão revelar-se determinantes no desenrolar da investigação.

Sobre a "imagem", são posteriormente efectuadas pesquisas com o objectivo de identificar evidências digitais (ficheiros e outro tipo de artefactos), relacionados com os

factos sob investigação. Conforme estas evidências vão sendo encontradas, devem ser extraídas, restauradas quando necessário (caso estejam danificadas ou cifradas), documentadas e devidamente preservadas. Em seguida, as evidências encontradas devem ser correlacionadas, permitindo a reconstrução dos eventos relacionados com o crime praticado. Muitas vezes, na análise das evidências, ao correlacionar e reconstruir os passos seguidos pelo criminoso, promove-se a descoberta de novas informações, formando um ciclo no processo de análise forense.

O recurso a métodos cientificamente comprovados para identificar evidências digitais, tem em vista facilitar ou promover a reconstrução de eventos no decurso da investigação, (Carrier, 2002).

Do ponto de vista dos tribunais, as evidências obtidas a partir de computadores devem incorporar todos os atributos das formas tradicionais de evidências, quer em termos de fiabilidade quer de admissibilidade. As evidências digitais apresentadas devem assim ser baseadas em conhecimentos cientificamente validados. Contudo, o estabelecimento e validação do conhecimento científico leva o seu tempo. Mesmo quando estão em causa apenas pequenos ajustamentos ao conhecimento já estabelecido, o carácter exaustivo dos testes e a elaboração da documentação que, por sua vez, tem que ser submetida a revisão e subsequente publicação, consome uma fatia significativa de tempo. Acresce que, só depois de terminado este processo, estão reunidas condições para que se possa planear o desenvolvimento de procedimentos e ferramentas práticas, os quais têm também de ser exaustivamente testados (Sommers, 2010).

Trata-se, de um processo que exige um alto nível de compreensão da forma como os dispositivos funcionam, o que, tendo em conta a velocidade a que evolui a indústria de Tecnologias de Informação e a forma pela qual os novos produtos são disseminados socialmente, levanta sérios problemas às instâncias judiciais, dada a dificuldade em compatibilizar o ritmo do ciclo normal de testes de novos métodos forenses com o ritmo a que surgem novos dispositivos.

3.10. FONTES RELEVANTES DE INFORMAÇÃO

A procura de evidências num sistema computacional, faz-se através de um desfolhar minucioso das informações aí residentes, quer tomem a forma de dados em ficheiros ou em memória, apagados ou não, codificados, encriptados ou até danificados.

O conceito da ordem de volatilidade das evidências digitais determina que o tempo de vida de uma evidência digital varia de acordo como o local onde ela se encontra armazenada. As principais fontes de informação de um sistema computacional, são as seguintes (por ordem decrescente de volatilidade): (Farmer, Venema, 2005)

- Registos;
- Memória principal;
- Estado da rede;
- Processos em execução;
- Disco rígido;
- Dispositivos de armazenamento removíveis.

Quanto maior a volatilidade de uma informação, mais difícil se torna a sua extracção e menos tempo temos para a capturar. Entretanto, informações voláteis como o conteúdo da memória principal, o tráfego da rede e o estado do sistema operativo, podem ser capturadas com relativa facilidade e podem conter pistas valiosas a respeito de eventuais ilícitos praticados.

No que respeita à recolha, é de vital importância que o investigador procure iniciar o processo a partir dos dispositivos mais voláteis, para os menos voláteis, e dos mais críticos, para os menos críticos. Por outro lado, há que atender ao facto de determinadas evidências apenas existirem enquanto o equipamento estiver em funcionamento, pelo que o equipamento não deverá ser desligado da rede eléctrica enquanto não for assegurada a recolha da informação residente nesses dispositivos.

3.10.1. REGISTOS

A permanência máxima de um dado num registo do processador pode ser tão curta como um único ciclo de relógio, tornando praticamente inviável capturar qualquer informação aqui residente, o que não constitui contrariedade de monta para a investigação, dado o fraco contributo que a informação ali residente pode acrescentar.

3.10.2. MEMÓRIA PRINCIPAL

A informação permanecerá na memória principal apenas enquanto o dispositivo permanecer ligado à corrente e não ocorra nenhum evento que, directa ou indirectamente, provoque algum tipo de perturbação (pico de corrente, comando

específico, etc.). Em situações particulares e recorrendo a hardware apropriado, é ainda possível ler o conteúdo da memória volátil após o dispositivo ter sido desligado, (Gutman, 2001).

O tipo de informação que pode ser obtido a partir da memória principal, ajuda a determinar o que pode ter ocorrido durante um determinado incidente. Poderemos encontrar: time-stamps do sistema, user(s) conectado(s), conteúdo da área de transferência, histórico de comandos, informações de serviços, drivers e processos em execução, bem como o estado do sistema operativo.

Capturar a memória principal, é um processo relativamente simples, porém, esta acção altera por si só o estado da memória, podendo a reconstrução das informações capturadas exigir conhecimento especializado. Nos processos de investigação, por norma, apenas pretendemos pesquisar determinados dados por palavras-chave, pelo que, nesta circunstância, não são requeridas habilidades especiais.

3.10.3. ESTADO DA REDE

O estado da rede está intimamente relacionado com os processos actuais que estão presentes num dispositivo electrónico, os quais, podem ser continuamente alterados. A análise do estado da rede pode permitir investigar não só actos de intrusão como avaliar a "teia" de interacções de um dado dispositivo e/ou individuo com outros, quer interna quer externamente.

3.10.4. PROCESSOS EM EXECUÇÃO

Os processos em execução encontram-se na memória principal, sendo que a sua execução termina quando o programa a que estão associados terminar ou for desligado o sistema. Relativamente aos processos, é conveniente estar alerta para a possibilidade da existência de processos automatizados, como parte da execução de uma aplicação ou inicialização de um serviço, bem como, a forma como estes podem afectar quer o estado da memória principal quer o estado de outras áreas do sistema.

Alguns processos podem constituir evidência de actividades não autorizadas, devendo todos eles ser verificados, pois podem esconder a presença de “Trojans”.

3.10.5. DISPOSITIVOS DE ARMAZENAMENTO

No que respeita ao crime económico, em grande parte das investigações é neste tipo de dispositivos que se encontra a maioria das provas. Para além da totalidade dos ficheiros

existentes no sistema, podemos recuperar uma quantidade significativa de informação não acessível através do sistema de ficheiros, nomeadamente ficheiros ou fragmentos de ficheiros que tenham sido entretanto apagados, ou até informação premeditadamente gravada em áreas não acessíveis (Carrier, 2005).

3.11. TÉCNICAS E FERRAMENTAS BASE MAIS UTILIZADAS

A sistemática evolução da tecnologia obriga à constante revisão das técnicas adoptadas para a recolha e tratamento de evidências digitais, condicionando o estabelecimento de uma metodologia estável e obrigando ao domínio de muitas e diferentes técnicas, o que torna esta actividade extremamente exigente.

3.11.1. PROCESSO DE AQUISIÇÃO

A facilidade com que uma evidência digital pode ser adulterada durante o processo de análise, aconselha a que este processo seja efectuado sobre uma cópia e não sobre o dispositivo original. Tirando partido da facilidade de duplicação com exactidão deste tipo de evidências, a realização de uma cópia do dispositivo suspeito constitui uma das primeiras acções a desenvolver antes de iniciar o processo de análise, preservando assim a integridade das evidências. O processo de aquisição poderá recorrer a uma de duas técnicas disponíveis: Aquisição Física ou Aquisição Lógica.

3.11.2. AQUISIÇÃO FÍSICA /LÓGICA – IMAGEM PERICIAL

O processo de aquisição física, realiza-se tipicamente ao mais baixo nível de abstracção operando uma transferência de toda a informação residente no dispositivo, que assegura a cópia exacta deste, preservando, para além dos ficheiros e estruturas de directório, todos os dados latentes que o dispositivo possa conter, "bit-stream-image", (Brown, 2006). O processo de aquisição lógica realiza-se a um nível de abstracção alto e, tipicamente, consiste na cópia de unidades lógicas de armazenamento, tais como ficheiros, para um suporte seguro.

Para garantir a preservação da integridade dos dados existentes no dispositivo do qual pretendemos uma imagem é comum recorrer a dispositivos de bloqueio de escrita "Write Blockers", no sentido de impedir qualquer acção de escrita no dispositivo alvo, o que pode acontecer pelo facto dos sistemas operativos executarem acções de forma automática, como por exemplo a indexação dos ficheiros, alterando, necessariamente, os respectivos "*time stamps*".

Constituindo a Aquisição Física (Bit Stream Image), uma das operações base da Informática Forense, iremos, na componente empírica da dissertação, confirmar a seguinte hipótese:

H1 – Existem ferramentas *Open Source* que permitem obter resultados iguais aos obtidos pelas ferramentas proprietárias na realização de imagens "Bit Stream" de um dispositivo de armazenamento.

3.11.3. FILE CARVERS

São ferramentas concebidas para a recuperação de ficheiros apagados. Através de um rastreio ao disco este tipo de ferramentas faz o levantamento dos blocos de informação não pertencente aos ficheiros existentes no sistema de ficheiros e, com base nas assinaturas conhecidas, de Cabeçalhos e Rodapés (*Headers and Footers*), combinam os blocos encontrados restaurando os ficheiros originais (Richard e Roussev, 2005).

3.11.4. HASHING

Para identificar rapidamente um ficheiro e para garantir que uma imagem ou ficheiro não foram modificados, a comunidade forense adoptou funções HASH, tirando assim partido das características deste tipo de funções, que permitem gerar uma cadeia de caracteres de tamanho fixo, *message digest,* a partir de uma sequência de qualquer tamanho.

O MD5 foi desenvolvido em 1991 por Ron Rivest e foi rapidamente adoptado para este efeito. Não obstante o National Institute for Standards and Technology [NIST] ter decidido adoptar como padrão o SHA-1, (FIPS 1995), a comunidade forense continuou a usar MD5 na maioria dos instrumentos, por ser mais rápido e produzir uma chave mais curta. Em 2004, porém, pesquisadores chineses, demonstraram insegurança no MD5 (Wang, et al, 2004), tornando questionável a sua utilização isolada, em contexto legal, passando a ser frequente a utilização cumulativa do MD5 e SHA1.

3.11.5. DATA REDUCTION

Um dos objectivos primordiais da investigação no campo da Informática Forense, é encontrar melhores e mais eficientes formas de descobrir evidências, no meio da informação contida nos dispositivos de armazenamento. O sistemático aumento da capacidade destes dispositivos a que se vem assistindo nos últimos anos constitui uma relevante contrariedade.

Na tecnologia digital, a representação de um carácter ocupa um byte. Considerando que, em regra, uma página tem cerca de 2.000 caracteres (média razoável para uma página em espaço duplo), chegamos ao valor 2Kb por página.

Naturalmente que, estes valores são apenas válidos para texto simples sem qualquer formatação, contudo, permitem estabelecer uma relação entre a ordem de grandeza da capacidade de armazenamento dos suportes digitais e o volume dos documentos que os mesmos podem comportar em termos de páginas dactilografadas.

Há cerca de uma década, a medida base para a capacidade dos suportes de armazenamento, era o Megabyte. 1 MB = 2^{20} Bytes = 1.048.576, correspondendo a cerca de 500 páginas; Passou entretanto a ser o Gigabyte. 1 GB = 2^{30} Bytes = 1.073.741.824, correspondendo a cerca de 500.000 páginas; Presentemente começa a ser comum encontrar equipamentos pessoais com unidades de armazenamento da ordem dos Terabytes. 1 TB = 2^{40} Bytes = 1.099.511.627.776, correspondendo a cerca de 500.000.000 páginas;

Podemos assim ter numa simples e comum Pendrive USB de 4 Gb 2 milhões de páginas de texto. Procurar uma evidência nesta imensidão de páginas constitui uma tarefa complexa, que consome muito do escasso tempo de que os investigadores dispõem para a investigação.

Para atenuar este problema, o NIST desenvolveu o projecto National Software Reference Library (NSRL, 2003), no âmbito do qual, criou uma Biblioteca Nacional de Referência de Software, projectada para recolher software das mais variadas fontes e incorporar perfis dos respectivos ficheiros numa Reference Data Set (RDS) de informação. O RDS constitui, assim, uma colecção de assinaturas digitais de aplicações de software conhecidas e rastreáveis. Actualmente esta base de dados contém perfis de ficheiros respeitantes a mais de 11.000 aplicações.

A vantagem de recorrer a este mecanismo consiste no facto de poder ignorar todos os ficheiros cuja assinatura (HASH) se encontra nesta base de dados, reduzindo assim de forma significativa o universo a analisar.

3.12. OPEN SOURCE NA INFORMÁTICA FORENSE

Em Informática Forense as ferramentas têm em vista a análise de informação digital, com o objectivo de incriminar ou ilibar alguém da suspeita de prática de actividades

ilegais, pelo que, o habitual confronto *Open Source* vs *Closed Source* não se resume, neste caso, a meras questões filosóficas, custos ou segurança. No contexto da Informática Forense, este confronto assume um carácter mais sério, mais centrado na fiabilidade dos resultados disponibilizados pelas ferramentas. É fundamental avaliar até que ponto as ferramentas cumprem os requisitos legais que regem a admissibilidade da prova.

No artigo *Gatekeeping Out Of The Box: Open Source Software As A Mechanism To Assess Reliability For Digital Evidence*, publicado no Virginia Journal of Law and Technology Association, Kenneally (2001), escalpeliza de forma bastante abrangente esta dicotomia e respectiva envolvência no meio judicial, concluindo que possibilitar o acesso sem restrições ao código das próprias ferramentas confere, neste contexto, uma significativa vantagem ao *open source*, face às "caixas negras" proprietárias.

4. RECOLHA DE PROVA

Antes de desenvolver um modelo ou uma teoria, é importante entender os requisitos do domínio no qual o modelo ou a teoria vai ser usado. O propósito final da análise efectuada no âmbito da Informática Forense é ajudar a encontrar e condenar os autores de um dado crime, pelo que, é fundamental entender, ainda que superficialmente, o contexto em que se insere.

Este capítulo começa por assegurar esse enquadramento. De seguida, caracteriza-se a forma como a informação digital é armazenada, procurando evidenciar as principais debilidades dos sistemas aproveitadas para ocultação de informação.

4.1. A NATUREZA DOS LITÍGIOS RESOLVIDOS NOS TRIBUNAIS

Os litígios que são resolvidos nos tribunais envolvem duas partes:

- uma que alega a ocorrência, no passado, de certos factos, em desconformidade com a lei vigente (acusação);

e

- outra que tentará refutar aquela acusação (réu ou acusado).

Se os factos em disputa constituírem violação do direito material por parte dos acusados, o litígio será criminal. Caso contrário, será civil.

Para resolver uma disputa, o tribunal deve primeiro estabelecer os factos necessários e, em seguida, aplicar-lhes a lei para tomar uma decisão. Entre os factos que necessitam de provas contam-se:

- os factos em questão, factos sobre os quais as partes em disputa discordam;
- os factos circunstanciais, cuja existência pode ser usada para provar ou refutar os factos em questão;
- os factos que devem ser provados para que a lei adequada possa ser aplicada ou que contribuam para demonstrar a relevância das evidências, de modo a assegurar a respectiva admissibilidade em processo judicial.

As evidências digitais, identificadas com recurso a ferramentas e metodologias associadas à Informática forense, podem revelar-se de extrema utilidade para suportar quaisquer destes três tipos de factos.

4.2. PAPEL DO COMPUTADOR NO CONTEXTO DO CRIME

O envolvimento de um computador ou dispositivo electrónico equiparável (Laptop, Netbook, PDA, Smart Phone, etc.) num crime, pode ocorrer segundo uma das seguintes formas:

1. O próprio dispositivo é o alvo do crime;
2. O dispositivo assume o papel de instrumento do crime;
3. O dispositivo constitui-se como repositório de evidências que permitem documentar o crime.

Podemos imaginar crimes de natureza económica em qualquer destes cenários. Um ataque ao "coração" de uma importante Praça Financeira pode ser concretizado elegendo como alvo o sistema informático que suporta a respectiva Bolsa de Valores. Partindo do princípio que o ataque é feito a partir de um outro sistema informático, teremos no mesmo caso os dois primeiros cenários. Contudo, para uma parte significativa dos crimes de natureza económica, o papel mais comum é o referido no terceiro cenário, em que o computador assume o papel de mero repositório de evidências. Será este o cenário escolhido para dissecar no presente trabalho.

4.3. NATUREZA DA INFORMAÇÃO

A informação existente num sistema informático divide-se em duas categorias distintas:

- Registos gerados pelo computador, englobando um vasto conjunto de artefactos que o sistema gera e mantém para seu próprio controlo, como: ficheiros de log de diversas naturezas e para diversos fins, ficheiros de "registry", ficheiros de histórico, ficheiros de link e Cookies, entre outros;

- A generalidade dos ficheiros criados e armazenados pelos utilizadores, tais como documentos produzidos por diversas aplicações, (processadores de texto, folhas de cálculo, etc.), aos quais ficam associados meta-dados que podem revelar-se de extrema utilidade para a investigação.

De uma forma geral, para que uma prova seja admitida em tribunal, é necessário demonstrar a sua autenticidade e fiabilidade. Nos EUA, a lei admite como autênticos os registos gerados pelo computador, desde que os programas que os geram estejam a funcionar correctamente, considerando, por outro lado, "hearsay evidences" ou seja evidências indirectas equiparadas a "Testemunhos de ouvir dizer" todos os registos

armazenados. Esta regra admite no entanto excepções, uma das quais relativamente aos documentos relacionados com a actividade económica das empresas, dado o carácter cíclico e regular com que os documentos são produzidos, acompanhando a dinâmica da actividade. É contudo frequente, que a prova digital assuma no processo um papel de complementaridade, reforçando ou fundamentando outro tipo de prova produzida, (Hoey A. 1996).

No que respeita aos países da União Europeia, um estudo levado a cabo em 16 Estados-membro, entre os quais Portugal, publicado em 2006 pelo Journal of Digital Forensic Practice, revelou que em nenhum deles a legislação faz qualquer referência ao termo "Evidência Electrónica", nem estipulam nas suas normas legais, uma definição específica do que entendem por provas electrónicas, sendo a referência mais directa encontrada no "Police & Criminal Evidence Code" do Reino Unido, referindo: "*evidências são todas as informações contidas num computador*." (Insa, 2006).

Neste conjunto de países, o tratamento dado à evidência electrónica é equivalente ao tratamento dado aos restantes tipos de evidência, sendo expressamente referidos três tipos de equivalências: (Insa, 2006)

- A equivalência entre documentos electrónicos e documentos em suporte papel, é a referência mais comum;
- A equivalência entre a assinatura electrónica e a assinatura manual, bem como entre o reconhecimento notarial electrónico e o reconhecimento notarial tradicional;
- A equivalência entre correio electrónico e correio postal.

4.4. SISTEMAS DE ARMAZENAMENTO DE INFORMAÇÃO

Restringindo o tipo de crimes de natureza económica, abordados neste estudo, àqueles para os quais o computador desempenha o papel de mero repositório de evidências, a unidade de disco rígido emerge como elemento nuclear, tornando-se indispensável uma abordagem detalhada ao seu funcionamento quer ao nível físico quer lógico.

Os sistemas de armazenamento da maioria dos dispositivos digitais têm sido desenvolvidos com preocupações de escalabilidade e flexibilidade, sendo projectados em camadas, o que se revela muito conveniente para definir os diferentes tipos de análise (Carrier, 2003a)

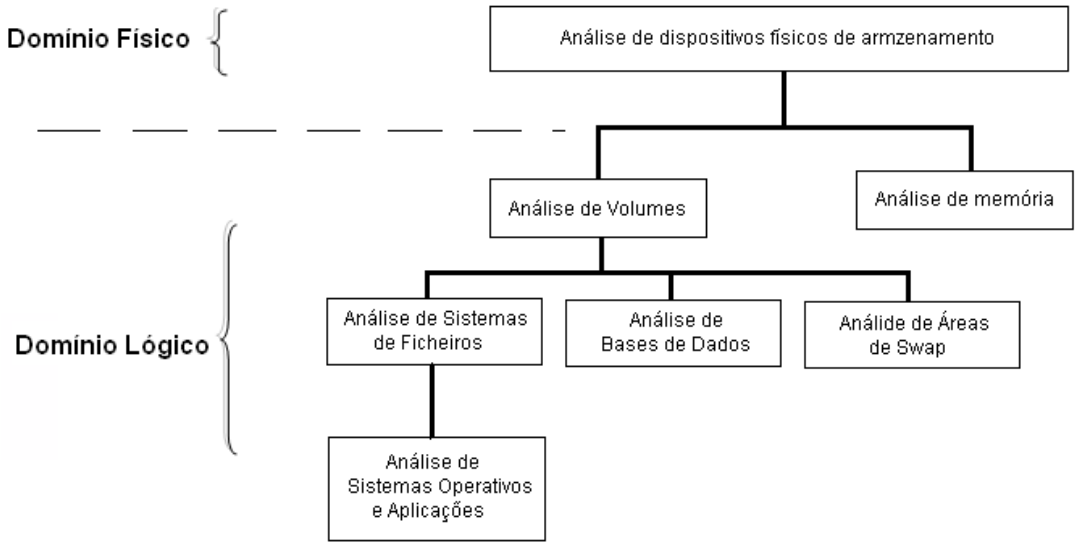

Figura 3 *- Camadas de análise com base na estrutura de dados, adaptado de (Carrier 2005)*

4.4.1. DISCO RÍGIDO

O Disco rígido serve como um meio de armazenamento não volátil constituindo repositório de documentos, ficheiros e aplicações. Com o surgimento do computador pessoal, passou a ser prática comum o sistema operativo (o software que interage directamente com o hardware fornecendo funcionalidades, quer para outros programas, quer para o próprio utilizador final), arrancar a partir de informações armazenadas num disco rígido (Start up).

Dada a riqueza das informações que podem estar armazenadas num disco rígido, é importante que o investigador tenha suficientes conhecimentos sobre a forma como os dados podem ser armazenados e ocultados nestes dispositivos.

Embora algumas aplicações de análise forense permitam automatizar o processo para identificar e recuperar informação a partir de uma dada unidade de disco rígido, existirão sempre situações não compatíveis para as quais é fundamental que o investigador esteja ciente dos atributos únicos e das subtilezas que caracterizam as unidades de disco rígido, bem como da forma como as informações podem ser armazenadas nestas unidades.

4.4.2. ORGANIZAÇÃO DOS DADOS

O armazenamento de dados em formato digital exige prévia atribuição (Allocation) de um espaço num dispositivo de armazenamento. Um byte é a menor quantidade de espaço normalmente atribuído, podendo comportar apenas 256 valores distintos. Na

prática, os bytes são normalmente agrupados, para poder armazenar uma maior diversidade de valores.

Muitas vezes o investigador é obrigado a analisar dados em bruto recorrendo a um editor hexadecimal. Nesses casos, é fundamental conhecer a ordem pela qual os números multi-byte são armazenados em memória pelo sistema em análise, pois esse armazenamento pode ser feito segundo as ordens "Little Endian" ou "Big Endian".

Com Little-Endian, o byte menos significativo é armazenado primeiro. Contrariamente, em Big-endien, é armazenado o byte mais significativo em primeiro lugar.

A figura abaixo mostra um valor de 4 bytes (0x12345678), para o qual foi previamente atribuído (allocated) um slot de 4 bytes, que começa no byte 80 e termina no byte 83, armazenado segundo os dois tipos de ordenação: little e big endian. (Carrier, 2005).

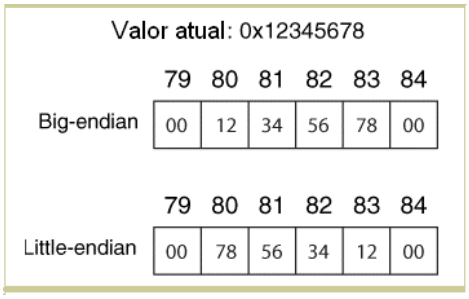

Figura 4 *– Representação ENDIAN , adaptado de (Carrier 2005)*

Ao analisar um sistema, é fundamental manter a respectiva ordem "endian" em mente, sob pena de vir a calcular valores incorrectos. Sistemas baseados na arquitectura IA32 (Intel Pentium) e correspondentes de 64 bits, usam little-endian. Sistemas baseados na arquitectura Sun SPARC e Motorola PowerPC (computadores Apple) usam big-endian.

4.4.2.1. VOLUMES

Os Dispositivos utilizados para armazenamento não volátil, são normalmente organizados em volumes. Um volume é uma colecção de locais de armazenamento endereçáveis, nos quais um utilizador ou aplicação podem escrever e ler. Existem dois conceitos importantes nesta camada. Um deles tem a ver com o particionamento, que permite a divisão de um volume em múltiplas partições independentes, e o outro com a montagem, através da qual podemos combinar vários volumes físicos num volume lógico maior, podendo este ser mais tarde particionado. (Carrier, 2005).

Alguns dispositivos de armazenamento, tais como disquetes, não têm quaisquer dados nesta camada, constituindo todo o disco um único volume.

A análise dos dados ao nível do volume é fundamental, pois permite-nos determinar onde estão localizados quer o sistema de ficheiros (file system), quer outros dados, bem como, determinar onde podemos encontrar dados ocultos.

Embora possamos ter qualquer tipo de dado dentro de cada volume (uma base de dados, espaço para troca temporária, *Swap space*, etc.), o mais comum é a existência de um sistema de ficheiros (file system).

4.4.2.2. PARTIÇÕES

Volumes e Partições têm muito em comum e podem mesmo ser confundidos. Contudo, existe uma subtil diferença entre estas duas entidades, que tem a ver com a contiguidade. Contrariamente ao volume, em que os sectores podem não ser contíguos, dado que podemos ter volumes que abarcam mais do que uma unidade física, as partições definem-se como um conjunto de sectores consecutivos existentes num volume.

Existem diversos cenários que justificam a existência de partições, destacando-se:

- Alguns sistemas de ficheiros impõem um tamanho máximo às unidades de armazenamento, que é menor do que a capacidade dos discos físicos;
- Muitos laptops usam uma partição especial para armazenar o conteúdo da memória quando o sistema entra em "*sleeping mode*";
- Nos sistemas UNIX é comum usar partições distintas em diferentes directórios, para minimizar o impacto, em caso de corrupção do sistema de ficheiros;
- Os sistemas intel com múltiplos sistemas operativos, requerem partições separadas para cada um dos sistemas operativos instalados.

4.4.2.3. SISTEMA DE FICHEIROS - FILE SYSTEM

Um sistema de ficheiros é uma colecção de estruturas de dados que permite que uma aplicação possa criar, ler e gravar ficheiros. O propósito deste sistema, é organizar um volume vazio, para que possamos nele armazenar dados, os quais poderemos posteriormente recuperar. A sua análise permite-nos encontrar ficheiros, recuperar ficheiros apagados, e encontrar dados ocultos. A função do sistema de ficheiros revela-se assim fundamental para correlacionar um nome de ficheiro com o respectivo

conteúdo. Portanto, quer o nome, quer a localização em disco, do conteúdo do ficheiro, são essenciais. O resultado da análise do sistema de ficheiros, pode ser o conteúdo de um ficheiro, como pode ser um conjunto de fragmentos de dados e meta-dados associados a ficheiros, (Carrier, 2005).

Para entender o que está dentro de um ficheiro, precisamos da camada de aplicação. A estrutura de cada ficheiro é baseada na aplicação ou sistema operativo que o criou. Por exemplo, na perspectiva do file system, um ficheiro de registo do Windows, não é diferente de uma página HTML, dado que são ambos ficheiros. Contudo, internamente, eles têm estruturas completamente diferentes e são necessárias diferentes ferramentas para analisar cada um deles, (Carrier, 2005).

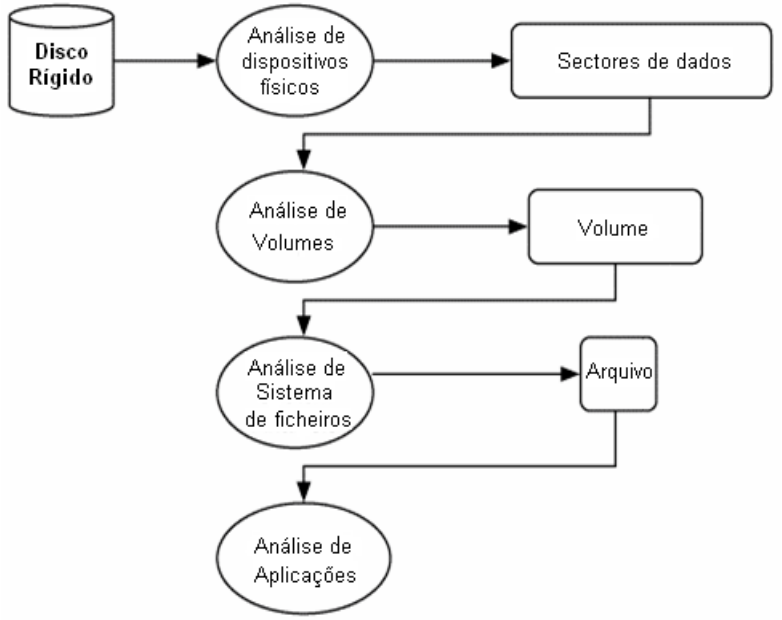

Figura 5 *- Sequência de análise do nível físico ao nível aplicacional, adaptado de (Carrier, 2005.*

4.4.3. ÁREAS DE POTENCIAL OCULTAÇÃO – NÍVEL FÍSICO

Podemos encontrar fontes de evidências digitais em praticamente qualquer dispositivo electrónico que disponha de alguma capacidade de armazenamento digital. Uma análise do dispositivo permite revelar a existência de áreas críticas, onde podem ser deliberadamente escondidas evidências digitais.

4.4.3.1. HPA E DCO

Alguns discos rígidos dispõem de uma área reservada designada por Host Protected Area (HPA), destinada a armazenar informação do fabricante. É igualmente comum a

existência da Device Configuration Overlay (DCO), destinada a permitir ajustes à configuração do disco, nomeadamente, alterar o número de clusters disponíveis.

Estas áreas foram projectadas para serem protegidas da actividade do utilizador normal, não sendo afectadas por utilitários do sistema operativo (formatar, apagar), e não podendo ser acedidas sem o recurso a um programa especial que reconfigura o controlador, para possibilitar o acesso a todos os blocos físicos. Não é, no entanto, difícil escrever um programa para aceder a essas áreas, permitindo gravar ali dados e, posteriormente, retornar para os recuperar. (Berghel et al, 2006).

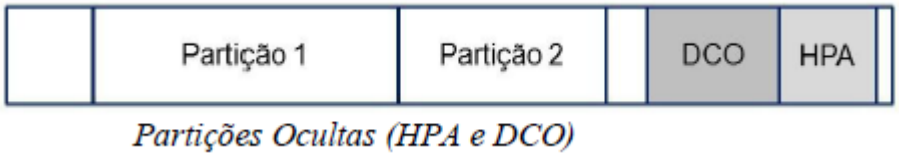

Figura 6 *– Host Protected Area e Device Configuration Overlay, adaptado de (Berghel et al, 2006)*

4.4.3.2. MBR E PARTIÇÕES EXTENDIDAS

Um disco rígido que contenha uma partição tipo DOS, tem obrigatoriamente espaço reservado no início da unidade para o Master Boot Record (MBR). Da conjugação do facto do MBR requerer apenas um único sector e as partições em regra começarem num limite de cilindro, resulta um desperdício de 62 sectores onde poderão ser escondidos dados. A necessidade de criar partições estendidas vai multiplicar estas áreas. (Berghel et all, 2006)

Figura 7 *– Espaço não utilizado no Master Boot Record ou partições estendidas, adaptado de (Berghel et al, 2006)*

4.4.3.3. VOLUME SLACK

As partições num disco rígido não utilizam a totalidade do espaço disponível, a área remanescente não pode ser acedida pelo sistema operativo por meios convencionais (por exemplo, através do Windows Explorer). Este espaço desperdiçado é chamado de Volume Slack. É também possível criar duas ou mais partições, nas quais se poderão gravar dados e, posteriormente, apagar, por exemplo, uma delas. Tendo em conta que o

acto de apagar a partição não vai afectar os dados, estes permaneceram ocultos (Berghel et al, 2006).

Figura 8 *– Volume Slack e Partições ocultas, adaptado de (Berghel et al, 2006)*

4.4.3.4. SECTORES / CLUSTERS

A unidade base de armazenamento de informação num disco é o sector, que, na maior parte dos sistemas, corresponde a 512 bytes. Contudo, a generalidade dos sistemas de ficheiros, não utiliza o sector como unidade de atribuição (allocated unit) de espaço em disco, dado o peso excessivo que tal representaria em termos de gestão (gerir uma unidade de disco com 20 GB com base em sectores de 512 bytes, implicaria gerir 40 milhões de sectores específicos).

Para tornar mais eficiente a gestão, os sistemas de ficheiros atribuem os sectores em blocos contíguos, designando estes blocos por clusters.

Um cluster é assim definido como a unidade base de atribuição de espaço de armazenamento ao nível do sistema de ficheiros, sendo constituído por um grupo de sectores consecutivos. O tamanho do cluster (número de sectores que abarca), varia com o dispositivo de armazenamento e é fixado no momento da formatação (Berghel et al, 2006).

4.4.3.5. PARTITION SLACK

Vimos que o sistema de ficheiros atribui dados em blocos (ou clusters). Trata-se de um esquema de atribuição que permite gerir grandes quantidades de dados através de um menor número de referências. Este mecanismo tende a tornar o armazenamento e o acesso muito mais eficiente do que a referência por sector. No entanto, se o número total de sectores numa partição não for um múltiplo do tamanho do bloco, haverá alguns sectores, no final da partição, que não podem ser acedidos pelo sistema operativo. Este conjunto remanescente de sectores é referenciado como Partition Slack, constituindo mais uma área onde podem ser escondidos dados (Berghel et al, 2006).

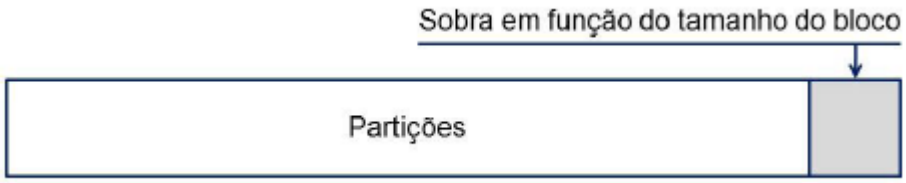

Figura 9 *– Partition Slack, adaptado de (Berghel et al, 2006.*

4.4.3.6. FILE SLACK

Todos os arquivos têm dimensão física e lógica. Geralmente a dimensão física é maior do que a dimensão lógica, sendo por vezes igual. Contudo, a dimensão lógica nunca deve ser maior que a dimensão física, caso contrário, estaremos em presença de um sistema de ficheiros corrompido.

A dimensão física de um ficheiro, é ditada pelo número mínimo de clusters inteiros de que ele necessita. Se por hipótese, a unidade base de atribuição do sistema de ficheiros for de 1 Cluster = 4KB, um ficheiro de 6 KB necessitará de 2 clusters físicos (8 KB), sendo que a sua dimensão lógica apenas irá ocupar 3/4 desse espaço, deixando 1/4 (2KB) sem utilização.

A dimensão lógica é o tamanho real do ficheiro que, neste caso, é de 6 KB. A diferença entre as duas dimensões é referenciada como "File Slack" e poderá também ser utilizada para dissimular dados (Berghel et al, 2006).

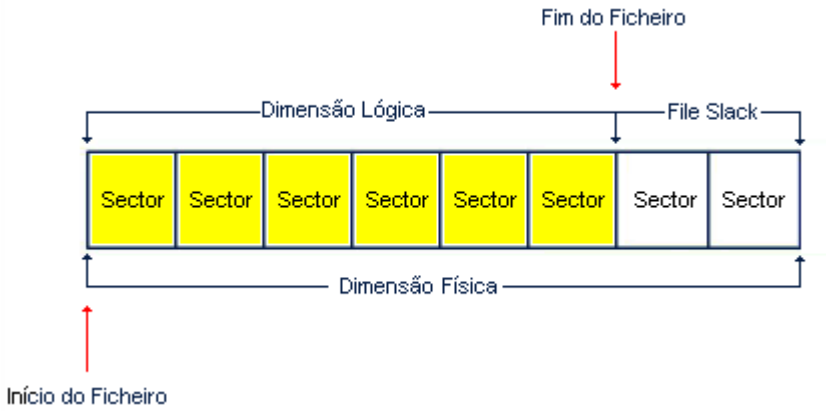

Figura 10 *– Espaço não utilizado no processo de gravação de dados, adaptado de (Berghel et al, 2006)*

4.4.3.7. BOOT SECTOR

Cada partição contém um sector de inicialização (boot), mesmo que a partição não seja inicializável. Os sectores de inicialização em partições não inicializáveis ficam assim disponíveis para esconder dados (Berghel et al, 2006).

Figura 11 *– Sectores de Boot não utilizados, adaptado de (Berghel et al, 2006).*

4.4.3.8. ESPAÇO NÃO ATRIBUÍDO

Qualquer espaço numa partição que não esteja atribuído a um ficheiro particular não pode ser acedido pelo sistema operativo. Até que esse espaço seja atribuído a um ficheiro, vai permitir ocultar dados.

É possível manipular os meta-dados do sistema de ficheiros que identificam os blocos danificados, por exemplo, a tabela de atribuição de ficheiros (File Allocation Table) num sistema de ficheiros FAT ou NTFS, de forma que, os blocos utilizáveis, sejam marcados como defeituosos, deixando assim de ser acedidos pelo sistema operativo. Deste modo produz-se um conjunto de blocos onde podem ser armazenados dados que passam despercebidos ao sistema operativo (Berghel et all, 2006).

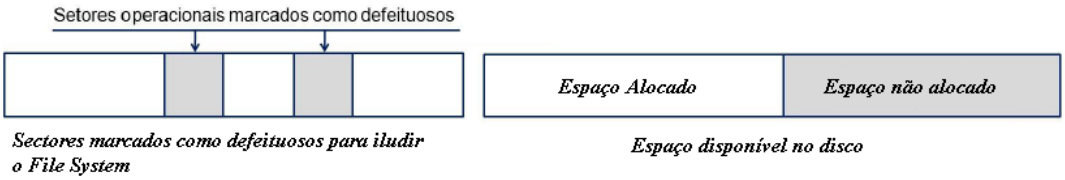

Figura 12 *– Espaço não alocado, adaptado de (Berghel et al, 2006)*

4.4.3.9. IMPACTO NA INVESTIGAÇÃO DO CRIME ECONÓMICO

Na investigação de crimes económico-financeiros, impõe-se a realização de um conjunto de tarefas chave, que permitam garantir a detecção das evidências procuradas, sempre que estas existam, contornando todos os obstáculos atrás referidos.

Na componente empírica deste trabalho serão efectuadas demonstrações nesse sentido cobrindo as seguintes áreas:

Recuperação de Partições: A investigação deste tipo de crimes envolve, por vezes, a análise de uma dada actividade ao longo de vários anos, sendo comum

deparar com dispositivos de armazenamento de informação colocados fora de serviço, e entretanto substituídos, nos quais pode existir informação relevante.

Na análise desses dispositivos são frequentes situações em que os dispositivos de armazenamento foram formatados, mostrando-se, nesses casos, necessário recuperar o respectivo conteúdo.

Em face deste tipo de cenário, relativamente frequente, será validada na parte empírica desta dissertação a seguinte hipótese:

H2 – Na investigação forense no campo digital, as ferramentas *Open Source* permitem obter melhores resultados na detecção e recuperação de volumes lógicos (partições).

Pesquisa por Palavra-Chave – Quando se parte para a análise de um equipamento, a equipa de investigação tem normalmente uma ideia do que procura, sendo comum fornecer uma lista de Palavras-Chave na qual se irá basear a análise, procurando assim, selecionar todos os elementos existentes no equipamento, quer em áreas acessíveis ao sistema de ficheiros, quer em espaço não atribuído (unallocated), que comportem alguma das Palavras-Chave da referida lista.

Neste âmbito, serão efectuados testes no sentido de confirmar a seguinte hipótese.

H3 – No que respeita a ferramentas para “pesquisa por palavra-chave”, as ferramentas *Open Source* disponíveis não estão ainda ao mesmo nível das ferramentas proprietárias.

Recuperação de ficheiros – A recuperação de ficheiros existentes em espaço não atribuído “unallocated space” é uma peça-chave na informática forense, pois consiste num rastreio integral de todo o dispositivo de armazenamento, realizado a baixo nível, no sentido de detectar e reconstruir a partir dos fragmentos encontrados, ficheiros anteriormente existentes no file system.

A esse propósito, serão efectuados testes no sentido de validar a seguinte hipótese:

H4 – As ferramentas *Open Source* permitem a recuperação de ficheiros existentes nos espaços não atribuídos das unidades de armazenamento de forma mais eficaz do que as ferramentas proprietárias.

4.4.4. REPOSITÓRIOS DE EVIDÊNCIAS DIGITAIS – NÍVEL LÓGICO

Face à estatística relativa a Feveeiro de 2012, publicada pelo Global Stats, continua a ser claro o domínio dos sistemas operativos da Microsoft, no segmento dos postos de trabalho, razão pela qual, será essa a plataforma alvo da análise a desenvolver na parte empírica desta dissertação.

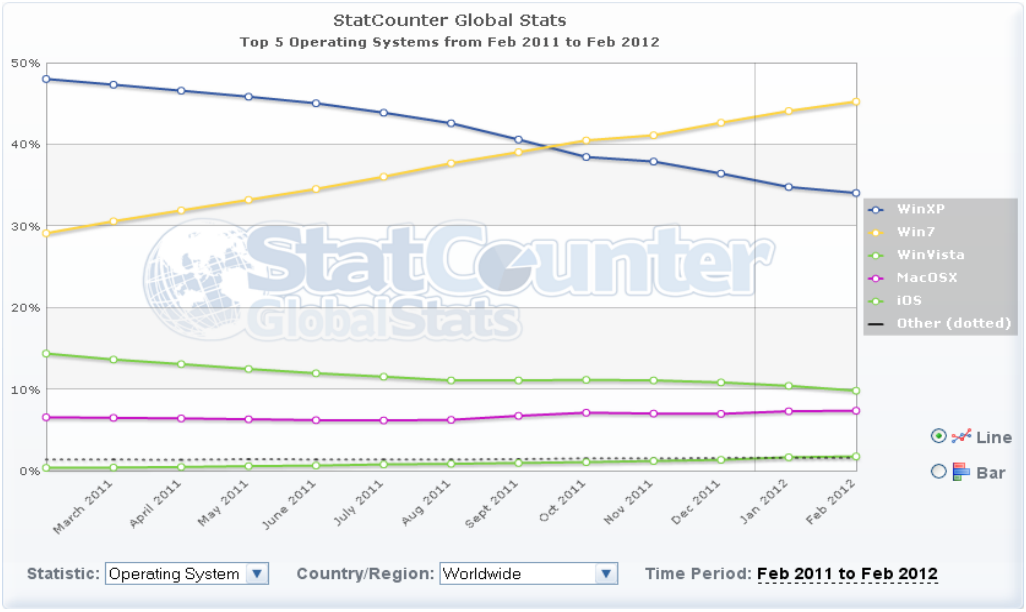

Figura 13 **–** OS Platform Statistics (StatCounter.com)

O Microsoft Windows disponibiliza inúmeros repositórios de evidências digitais que permitem a reconstrução dos eventos que ocorreram num dado equipamento. No momento em que o Microsoft Windows é instalado num computador, são criados diversos directórios e ficheiros especiais extremamente importantes para a investigação forense, no campo digital.

Começando pelo conhecimento das características dos dois tipos de file system adoptados pela Microsoft, FAT [2] e NTFS[3], indispensável para interpretar os múltiplos elementos que possamos recuperar, este Sistema Operativo faz uso de diversos ficheiros para registo de elementos com relevante interesse, como sejam:“Recycle Bin”, “Event Logs”, “Link Files”, “Swap file”, “Hibernation File”, Print Spooling”, “Registry”, entre outros, bem como, uma estrutura de directórios igualmente relevantes como: “*Recent*

[2] FAT File System - http://technet.microsoft.com/en-us/library/cc938438.aspx ;
[3] NTFS File System - http://technet.microsoft.com/en-us/library/cc976808.aspx;

Folder”, “My Documents”, “Temp Folder”, “Send To Folder”, “Favorites Folder”, “Cookies Folder”, “History Folder”, etc.

A análise destes directórios e ficheiros pode revelar-se determinante, quer para a identificação, quer para confirmação de elementos de prova.

Desde vasto conjunto de artefactos, tendo em conta o carácter exploratório deste trabalho, iremos destacar o "Registry" pela riqueza extrema de informações que este armazena, não apenas sobre a configuração, mas, sobretudo, acerca do uso que se faz do computador.

Naturalmente que a vastidão do “Registry” não permitiria que este fosse inteiramente escalpelizado neste trabalho, pelo que, apenas iremos debruçar-nos sobre alguns aspectos particulares, que darão lugar a mais uma análise na componente empírica da dissertação.

4.4.4.1. REGISTRY DO WINDOWS

O "Registry" apresenta-se, como um dos principais locais para recuperar diversas informações relacionadas com o sistema operativo, desde as aplicações que foram instaladas no equipamento, às informações sobre os utilizadores com acesso ao sistema, respectivas configurações e privilégios de que dispõem para interagir com aplicações e redes (Carvey, 2005; Sheldon, 2003).

Figura 14 – Hives do Registry

Ao visualizar o "registry" este apresenta um aspecto semelhante a uma estrutura de cinco pastas, designadas por "hives", cujos identificadores iniciam com os caracteres "HKEY". Contudo, destes cinco, apenas dois têm existência real: HKEY_USERS (HKU) e HKEY_LOCAL_MACHINE (HKLM), sendo os restantes meros links.

Cada um destes "hive", é constituído por "Chaves" as quais contêm "Valores" e "Sub-Chaves". Os "Valores" correspondem a nomes de certos items dentro de uma chave, os quais identificam de forma unívoca valores específicos relacionados com o sistema operativo, ou aplicações que dependem desses valores.

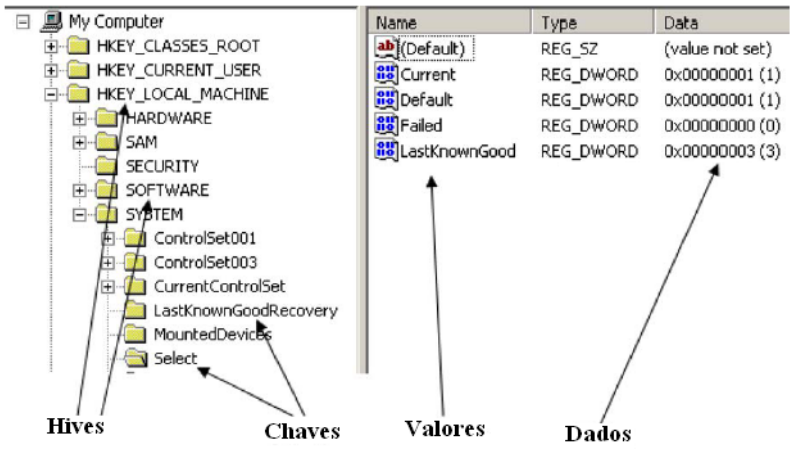

Figura 15 – Estrutura interna dos Hives do Registry

4.4.4.2. CHAVE MRU – "MOST RECENTLY USED"

Para evidenciar a qualidade do "registry" como repositório de evidências, observemos a chave MRU, que consiste numa lista dos items mais recentemente utilizados contendo entradas respeitantes a ações específicas executadas pelo utilizador.

Existem inúmeras MRU localizadas em diversas chaves de "registry". O "Registry" mantém estas listas de itens para o caso do utilizador voltar a usar os mesmos items no futuro. Trata-se de um mecanismo em tudo semelhante ao funcionamento dos cookies e histórico dos web browsers.

Um exemplo de uma MRU mantida no Registry do Windows é a chave RunMRU, que recolhe elementos relativamente aos comandos digitados pelo utilizador na caixa "Executar" existente no menu Iniciar, conforme exemplifica a figura.

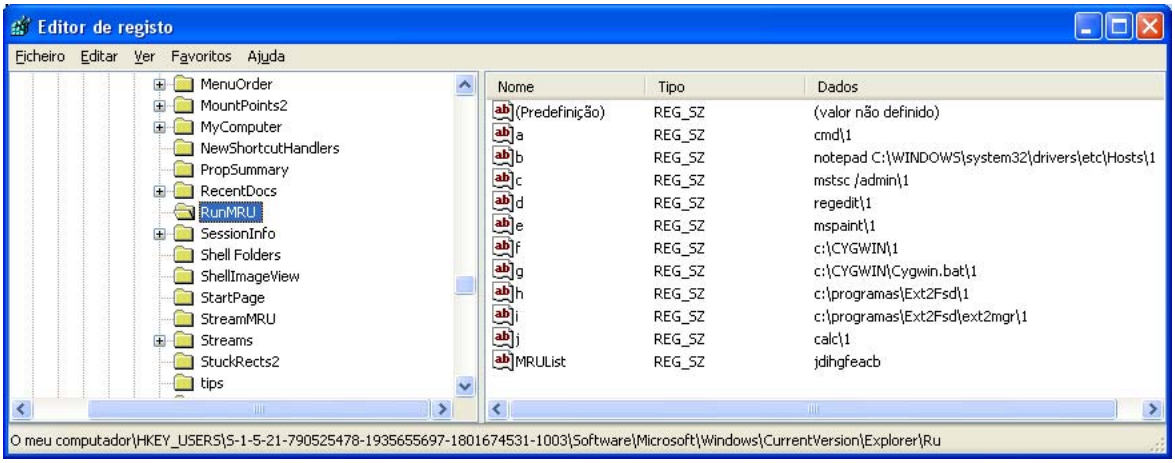

Figura 16 – Conteúdo da chave RunMRU

A ordem cronológica de aplicações executadas via "Executar" pode ser determinada olhando para a coluna de dados do valor MRUList. A primeira letra corresponde ao comando digitado na caixa "Executar" em último lugar. De acordo com a figura 16, trata-se da letra "j" à qual está associado o comando "calc" correspondente à aplicação Calculador do Windows. O valor LastWrite da chave RunMRU refletirá a data e a hora a que a entrada foi inserida na chave e, consequentemente, o momento em que o comando/aplicação associado(a), foi executado(a).

A informação fornecida pela chave RunMRU, pode revelar-se determinante para o esclarecimento de um crime, pois o examinador consegue reconstituir as acções desenvolvidas no sistema pelo suspeito, permitindo-lhe compreender melhor o respectivo comportamento.

4.4.4.3. CHAVE USBSTOR

Outro exemplo extremamente importante na investigação de crime económico, pode ser dado pela chave USBSTOR.

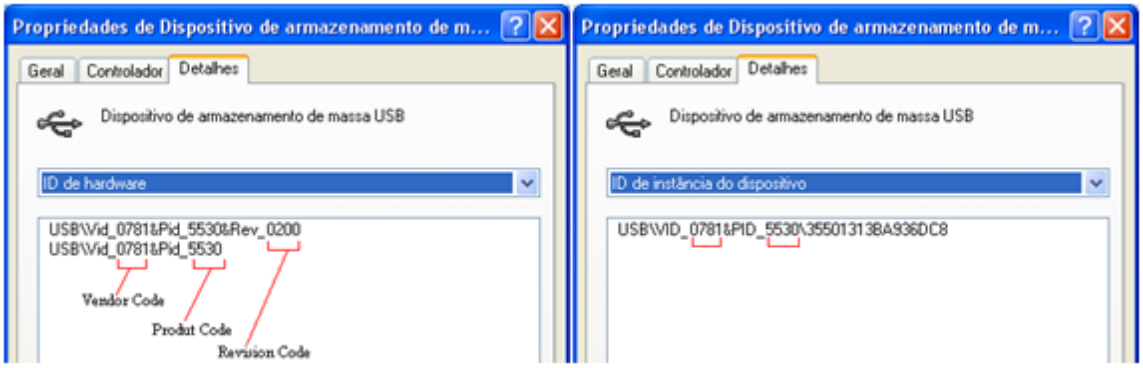

Figura 17 – Elementos do "Hardware ID" do dispositivo que integram o "Instance ID"

Todos os dispositivos USB integram informação associada ao respectivo fabricante, com base na qual o sistema operativo constrói um perfil único que é usado para identificar esses dispositivos. Estes identificadores são registados em diferentes locais do sistema, nomeadamente no “registry”, e tendem a ser persistentes após desligar o equipamento (Gorge, 2005).

Esta capacidade de preservar a informação sobre os dispositivos tem por objectivo reduzir o número de reinstalações sempre que o dispositivo é ligado ao sistema, e revela-se de extrema utilidade para a investigação.

No que respeita aos dispositivos USB, o "registry" do Windows armazena informações que asseguram o carregamento dos drivers apropriados ao respectivo funcionamento, e mantém o histórico das conexões sob a seguinte chave:

HKEY_LOCAL_MACHINE\System\ControlSet00x\Enum\USBSTOR

O ControlSet em uso pelo sistema, depende dos dados associados com o seguinte valor do "Registry"(Carvey, 2005):

HKEY_LOCAL_MACHINE\System\Select\Current

Cada dispositivo USB, actual ou previamente ligado ao sistema, tem o identificador de instância do dispositivo registado na chave USBSTOR de acordo com a figura.

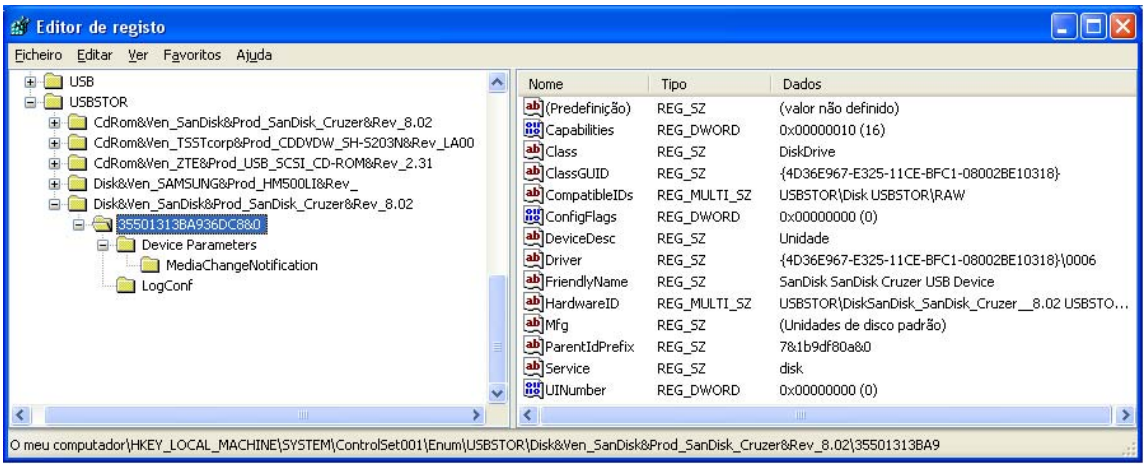

Figura 18. Vista do identificador único USB sob a chave de registry USBSTOR

Análise do “Registry” – A análise do “Registry” do Windows, revela-se assim incontornável, em grande parte das investigações. Através do registry, podemos encontrar a lista de contas de utilizadores; seguir o percurso de utilização de dispositivos de armazenamento móveis, através do histórico de dispositivos

conectados; analisar listas das URL's digitadas nos Web Browsers, bem como, obter informações sobre unidades de rede partilhadas, entre muitas outras informações de extrema relevância para a investigação.

Como forma de ilustrar a importância deste recurso, será realizada a análise de uma situação concreta envolvendo a identificação de uma unidade de armazenamento móvel, de modo a validar a seguinte hipótese:

H5 – Analisar o "registry" do Windows com ferramentas *Open Source* é possível e fornece resultados tão fiáveis como os obtidos com ferramentas proprietárias.

5. AMBIENTE DE ANÁLISE

Tendo em vista caracterizar o ambiente de análise, o presente capítulo, começando por uma abordagem teórica no sentido de justificar a necessidade de recorrer ao mecanismo de camadas de abstracção, procurará identificar e descrever as características de cada uma das ferramentas seleccionadas para assegurar o tratamento do caso prático, que será desenvolvido no próximo capítulo.

5.1. CAMADAS DE ABSTRACÇÃO

O problema da complexidade na análise forense digital, tem a ver com o formato em que se encontram os dados recolhidos, tipicamente no formato mais básico, que corresponde a uma sequência de zeros e uns, cuja compreensão se torna muito difícil para o ser humano.

Para resolver esta complexidade, são utilizadas ferramentas que permitem traduzir os dados através de uma ou mais camadas de abstracção, até que se atinja um patamar onde os mesmos possam ser entendidos.

***Figura 19** – Camada de Abstracção, adaptado de Carrier, (2003-B)*

Como exemplo básico desta realidade, pode apontar-se a tabela ASCII, que constitui uma camada de abstracção que estabelece uma correspondência entre cada um dos caracteres do alfabeto inglês, e um número entre 32 e 127. Quando gravamos um texto, os respectivos caracteres são convertidos no valor numérico correspondente, e gravado no dispositivo de armazenamento sob a forma de bits. A visualização deste ficheiro no seu formato base, mostrará uma simples sequência de zeros e uns ("0" e "1"). A aplicação da camada de abstracção que a tabela ASCII aqui representa, permitirá identificar cada caracter do texto, em função do respectivo valor numérico, possibilitando assim a sua leitura.

Podemos ter camadas de abstracção dentro de uma camada de abstracção de mais alto nível. No caso do armazenamento em disco, existem pelo menos quatro camadas de abstracção de alto nível:

- A primeira é a camada do meio físico, que traduz o formato específico da unidade de disco para os formatos standard LBA (Logic Block Addressing) e CHS (Cylinder-head-sector) de endereçamento que a interface de hardware fornece;
- A segunda é a camada de gestão do suporte, que traduz todo o disco para partições menores;
- A terceira é a camada do sistema de ficheiros, que traduz o conteúdo da partição para os ficheiros;
- A quarta é a camada de aplicação, que traduz o conteúdo dos ficheiros para as necessidades da aplicação.

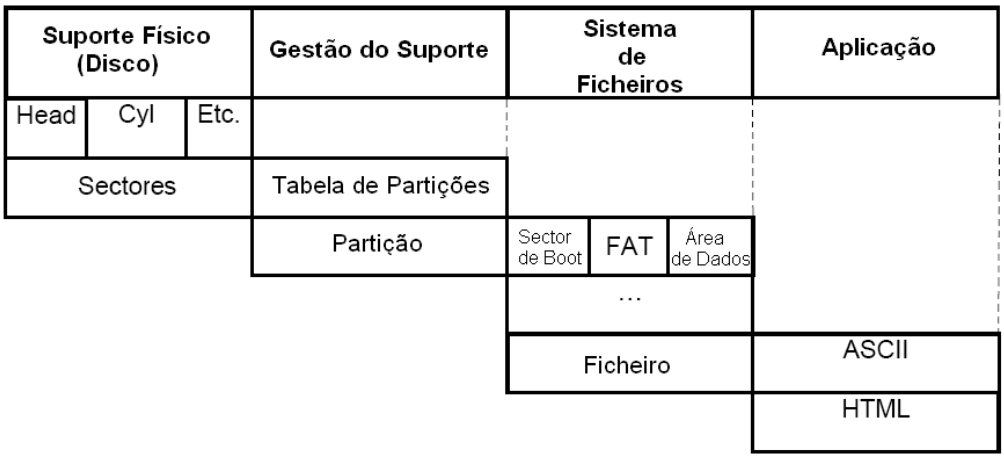

***Figura 20** – Níveis e camadas de abstracção de um arquivo HTML, adaptado de Carrier, (2003-B)*

Tendo por base o enquadramento estabelecido, é exigível um conjunto de requisitos, às ferramentas a utilizar no processo de análise (Brezinski e Killalea, 2002) :

- **Usabilidade** - Para resolver o problema da complexidade (dados no formato básico difíceis de analisar), as ferramentas devem ser capazes de disponibilizar os dados num formato claro e preciso, para que a respectiva interpretação não suscite dúvidas;

- **Abrangência** - Para identificar provas, quer de acusação quer de defesa, o investigador deve ter acesso à totalidade dos dados de saída de determinada camada de abstracção;
- **Precisão** - Para resolver problemas de eventuais erros introduzidos pelas camadas de abstracção, as ferramentas devem permitir calcular as margens de erro, de modo a assegurar que os dados de saída são exactos e que os resultados podem ser interpretados de forma apropriada;
- **Determinismo** - Para garantir a respectiva precisão, a ferramenta, em face do mesmo conjunto de regras e da mesma entrada, deve produzir sempre os mesmos resultados;
- **Verificabilidade** - A precisão da ferramenta deve ainda poder ser aferida, quer manualmente, quer recorrendo a uma outra ferramenta independente, sendo no entanto necessário o acesso às entradas e saídas de cada camada, de modo a que os resultados alcançados possam ser verificados.

5.2. DEFINIÇÃO DA PLATAFORMA DE ANÁLISE

O trabalho empírico a desenvolver terá por base uma plataforma de análise forense de evidências digitais, assente num conjunto de ferramentas de código aberto, capaz de dar resposta às situações mais comuns associadas ao processo de investigação de crimes económicos e financeiros. O facto de pretender recorrer a ferramentas "*open source*", confronta-nos com duas questões base:

- Uma parte significativa das ferramentas "*open source*" é distribuída em código fonte;
- Muitas das ferramentas, existem sob a forma de scripts, cuja execução exige um intérprete específico.

Face a esta realidade, a nossa plataforma de análise terá que dispor dos meios necessários não só para converter o código fonte em código executável (ambiente de desenvolvimento), como para assegurar a interpretação de scripts em diversas linguagens. Para isso, são indispensáveis diversos interpretadores, nomeadamente, Perl, Python e Ruby. Paralelamente, será ainda necessário assegurar a instalação de módulos específicos, que constituem requisitos básicos de algumas das aplicações a utilizar

como, por exemplo, as livrarias “libewf” e “afflib”, que possibilitam o acesso aos dois formatos específicos de contentores para armazenamento de imagens de unidades de armazenamento de informação, para uso forense: EWF (Expert Witness Format) e AFF (Advanced Forensic Format).

A plataforma de análise assenta sobre a distribuição Caixa Mágica 17, que utiliza já a release 3.0.0 do kernel Linux, e será descrita no anexo I da dissertação.

5.3. WRITE BLOCKERS

Para além da estação de trabalho, desktop ou portátil, é indispensável o recurso a unidade de bloqueio de escrita.

A preservação da integridade das evidências digitais é condição base para a admissibilidade destas em tribunal, pelo que, é fundamental garantir que as ações desenvolvidas ao longo do processo de análise tenham o menor impacto possível nos dispositivos analisados. O recurso a dispositivos de bloqueio de escrita "Write Blockers" é essencial para evitar que, inadvertidamente, possa ocorrer qualquer acção de escrita no dispositivo suspeito.

Figura 21 *– Bloqueadores de escrita*

5.4. DEFINIÇÃO DE HIPÓTESES: SÍNTESE

Ao longo do estudo teórico foram identificados os seguintes cenários e hipóteses associadas, comuns em processos de investigação de crimes de natureza económica:

1. **Aquisição Física** – Realização da imagem pericial (Bit Stream Image) de um dispositivo de armazenamento, de modo a validar a seguinte hipótese:

   H1 – Existem ferramentas *Open Source* que permitem obter resultados, iguais aos obtidos pelas ferramentas proprietárias, na realização de imagens “Bit Stream” de um dispositivo de armazenamento.

2. **Recuperação de Partições** – Perante um dispositivo de armazenamento no qual o sistema não detecta qualquer partição, serão desenvolvidas as acções necessárias para a respectiva recuperação, de modo a validar a seguinte hipótese:

H2 – Na investigação forense, no campo digital, as ferramentas *Open Source* permitem obter melhores resultados na detecção e recuperação de volumes lógicos (partições).

3. **Pesquisa por Palavra-Chave –** Realização de um procedimento de pesquisa por palavra-chave sobre uma imagem (Bit Stream) de um dispositivo de armazenamento, de modo a validar a seguinte hipótese:

   H3 – No que respeita a ferramentas para "pesquisa por palavra-chave", as ferramentas *Open Source* disponíveis não estão ainda ao mesmo nível das ferramentas proprietárias.

4. **Recuperação de Ficheiros a partir de espaço não atribuído** – Realização de um procedimento de recuperação de ficheiros a partir de espaço não atribuído (unallocated space), de modo a validar a seguinte hipótese:

   H4 – As ferramentas *Open Source* permitem a recuperação de ficheiros existentes nos espaços não atribuídos das unidades de armazenamento de forma mais eficaz do que as ferramentas proprietárias.

5. **Análise do "Registry"** – Realização de um procedimento de análise do registry, envolvendo a identificação de uma unidade de armazenamento móvel, de modo a validar a seguinte hipótese:

   H5 – Analisar o "registry" do Windows com ferramentas *Open Source* é possível e fornece resultados tão fiáveis como os obtidos com ferramentas proprietárias.

O conjunto de hipóteses formuladas tem por objectivo aferir a valia das ferramentas *Open Source* disponíveis no tratamento e análise das evidências digitais em cada um dos casos, face ao desempenho da ferramenta proprietária de referência "EnCase Enterprise".

Para tal, ao longo do próximo capítulo será realizado o trabalho empírico associado a cada um dos cenários, que consistirá na realização, em paralelo, dos procedimentos com uma ferramenta *Open Source* selecionada e a ferramenta proprietária de referência.

6. TRABALHO EMPÍRICO: APRESENTAÇÃO E VALIDAÇÃO DE RESULTADOS

O presente capítulo tem por objectivo a realização do trabalho empírico, que irá focar as fases de aquisição (realização de imagens periciais) de dispositivos de armazenamento de massa e a subsequente fase de análise, visando a recolha de prova digital.

Através deste trabalho, pretende-se demonstrar que uma parte significativa das tarefas de análise e recuperação de prova digital podem ser asseguradas com recurso a ferramentas *Open Source*, sem pôr em causa a respectiva integridade.

A metodologia adoptada consiste na realização de determinadas tarefas com recurso à plataforma proprietária de análise forense, "EnCase Enterprise", repetindo a realização das mesmas tarefas através da utilização de ferramentas *Open Source*, comparando em seguida os resultados obtidos.

6.1. "CENÁRIO-1_MOSS" – CRIAÇÃO DE IMAGENS PERICIAIS

De acordo com as recomendações do Software Working Group on Digital Evidence (SWGDE1, 2011.), a análise forense de dispositivos digitais deve ser efectuada sobre uma cópia integral do dispositivo original, conforme referido em 3.11.2, de modo a preservar o original de danos eventuais que a manipulação directa poderia provocar.

6.1.1. IMAGEM PERICIAL – UTILIZANDO "ENCASE"

O EnCase é um sistema integrado de análise forense baseado no ambiente Windows, desenvolvido pela Guidance Software INC.[4]. Trata-se de um software amplamente utilizado por profissionais das áreas da computação forense, segurança informática e e-discovery.

O processo utilizado pelo EnCase inicia-se com a abertura de um caso, recolhendo elementos de identificação da situação a analisar, e prossegue com a criação de imagens dos dispositivos (disquetes, Zips, Jaz, CDROM, DVDs, PenDrives, discos rígidos, etc.), relacionados com o caso. Cada caso pode envolver diversos dispositivos. Depois da criação das imagens, denominadas no EnCase por "evidence files" (contentores no formato EWF referenciado no anexo I em A.1-8- ***Figura A1-1***), permite prosseguir com a

[4] http://www.guidancesoftware.com/

respectiva análise, a qual poderá envolver todas as imagens de um dado caso, em simultâneo.

Dadas as características do ambiente Windows que, sempre que é acedido, escreve no disco rígido, alterando dados do sistema, o EnCase não opera directamente sobre o dispositivo original, montando em alternativa os "evidence files" como discos virtuais, protegidos contra escrita.

Deste modo o EnCase, substituindo o sistema operativo, reconstrói o sistema de arquivos contido em cada "evidence file", permitindo ao investigador visualizar, ordenar e analisar os dados, de forma não invasiva, através de uma interface gráfica que disponibiliza um vasto conjunto de funcionalidades de análise.

O dispositivo suspeito que, no âmbito do presente caso, será objecto de análise, é uma Pen USB de 1 GB, da qual se vai começar por criar uma imagem.

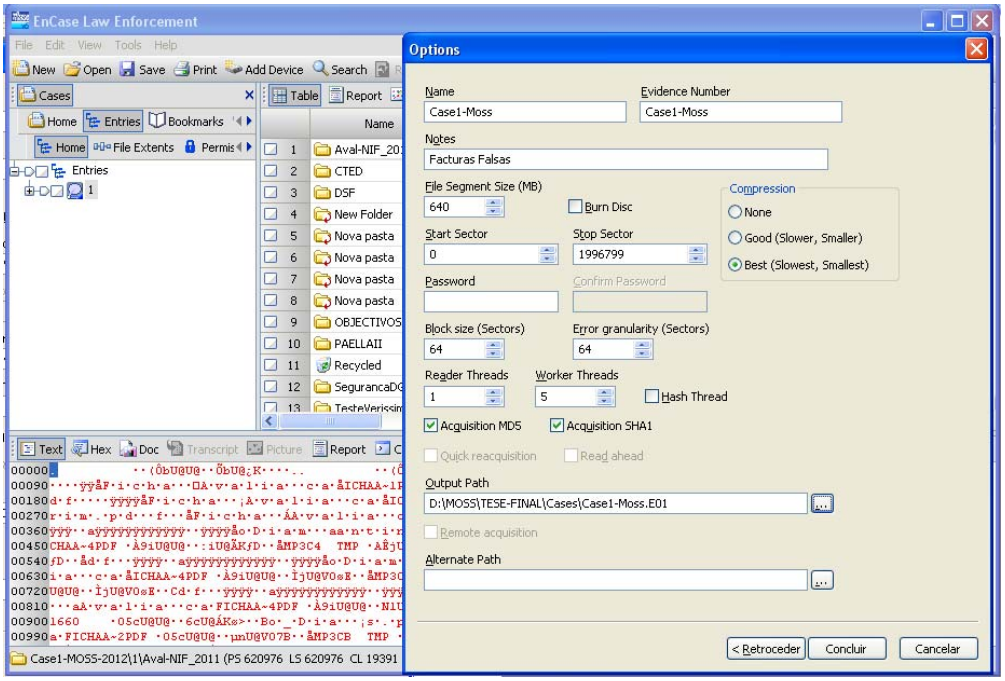

Figura 22 – Interface gráfica do EnCase, ferramenta "Acquire"

Conforme documenta a figura 22, o processo de criação da imagem disponibiliza um conjunto de opções, a saber:

- O particionamento da imagem em ficheiros de uma dada dimensão. No caso presente optou-se por fraccionar em ficheiros de 640 MB de modo a facilitar a respectiva gravação em CD-ROM.

- Dois níveis de compressão. Esta opção deverá ter em conta o *trade off:* mais compressão / maior rapidez. No caso presente, a opção escolhida foi "best" que correspondendo à taxa mais elevada de compressão, torna o processo de aquisição mais lento.

- No que respeita à certificação HASH, é possível selecionar o cálculo com base nos algoritmos MD5 e SHA, individual ou conjuntamente.

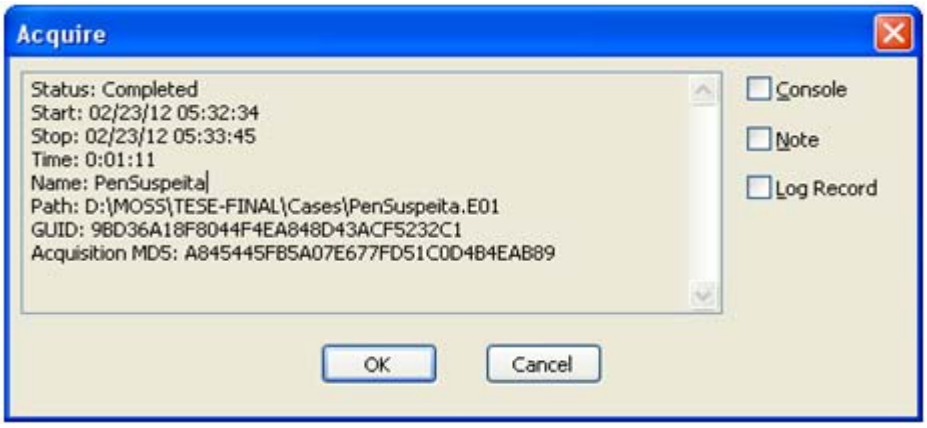

Figura 23 – Informação disponibilizada no final do processo

6.1.2. IMAGEM PERICIAL – UTILIZANDO "DD"

O comando "dd" é um comando base nos sistemas operativos da família Unix, existindo igualmente para os sistemas Windows, concebido para realizar cópia e conversão de ficheiros de um local para outro.

Dado que este comando permite realizar uma cópia integral bit a bit (RAW), do dispositivo alvo, reúne as condições necessárias para criar imagens destinadas a análise forense.

Contudo, apresenta algumas desvantagens, de que se destacam o facto de não possibilitar compactação, resultando em ficheiros de grandes dimensões, e de não permitir incorporar meta-dados que possibilitem a identificação do processo de investigação associado à imagem.

```
mdelgado@mdelgado-VirtualBox:~/MOSS/CaseStudy$ sudo dd if=/dev/sdb
of=/home/mdelgado/MOSS/CaseStudy/PenSuspeita.dd
[sudo] password for mdelgado:
1996800+0 registos dentro
1996800+0 registos fora
1022361600 bytes (1,0 GB) copiados, 207,381 s, 4,9 MB/s
```

Figura 24 – Realização da imagem com o comando "dd".

```
mdelgado@mdelgado-VirtualBox:~/MOSS/CaseStudy$ sudo md5sum
PenSuspeita.dd
[sudo] password for mdelgado:
a845445fb5a07e677fd51c0d4b4eab89  PenSuspeita.dd
```

Figura 25 – Cálculo do HASH da imagem criada com algoritmo MD5.

```
mdelgado@mdelgado-VirtualBox:~/MOSS/CaseStudy$ sudo md5sum /dev/sdb
a845445fb5a07e677fd51c0d4b4eab89  /dev/sdb
mdelgado@mdelgado-VirtualBox:~/MOSS/CaseStudy$
```

Figura 26 – Cálculo do HASH do conteúdo do dispositivo para confirmação.

6.1.3. IMAGEM PERICIAL – UTILIZANDO "EWFACQUIRE"

O "ewfacquire" é um utilitário *Open Source* integrado na livraria "LIBEWF", referida em 5.2, concebido para a aquisição de dados a partir de um dispositivo de armazenamento, (disquetes, Zips, Jaz, CDROM, DVDs, PenDrives, discos rígidos, etc.), gravando ficheiros no formato EWF (Expert Witness Compression Format), adoptado pelas plataformas proprietárias EnCase Forensic e Forensic Toolkit (FTK) Imager.

Este utilitário permite o particionamento da informação em ficheiros de dimensão controlada, possibilita a selecção, dentro da tipologia EWF, de subtipos associados a diversas plataformas e respectivas versões, bem como a compactação a diversos níveis e admite a incorporação de meta-dados para identificação do processo de investigação associando dados descritivos do dispositivo suspeito, identificação do perito, entre outros elementos.

```
VirtualBox:~$ sudo ewfacquire /dev/sdb
ewfacquire 20100226 (libewf 20100226, libuna 20091031, libbfio
20091114, zlib 1.2.3.4, libcrypto 1.0.0)
Media information:
Device type:                Direct access
Bus type:
Removable:          yes
Vendor:             JetFlash
Model:              TS1GJFV20
Serial:
Media size:         1.0 GB (1022361600 bytes)
```

Figura 27 – O comando começa por ler as características do dispositivo alvo.

```
Acquiry parameters required, please provide the necessary input
 Image path and filename without extension:
                    /home/mdelgado/MOSS/CaseStudy/PenSuspeita
Case number: Case1-MOSS
Description: Facturas Falsas
Evidence number: 001
Examiner name: M.Delgado
Notes: Pen USB 1 GB suspeita
Media type (fixed, removable, optical, memory) [removable]:
Media characteristics (logical, physical) [logical]: physical
Use compression (none, empty-block, fast, best) [none]: best
Use EWF file format (ewf, smart, ftk, encase1, encase2, encase3,
encase4, encase5, encase6, linen5, linen6, ewfx) [encase6]:
Start to acquire at offset (0 >= value >= 1022361600) [0]:
The amount of bytes to acquire (0 >= value >= 1022361600)
[1022361600]:
Evidence segment file size in bytes (1.0 MiB >= value >= 7.9 EiB)
[1.4 GiB]: 640 MiB
The amount of bytes per sector (0 >= value >= 4294967295) [512]:
The amount of sectors to read at once (64, 128, 256, 512, 1024,
2048, 4096, 8192, 16384, 32768) [64]:
The amount of sectors to be used as error granularity (1 >= value >=
64) [64]:

The amount of retries when a read error occurs (0 >= value >= 255)
[2]:
Wipe sectors on read error(mimic EnCase like behavior)(yes,no)[no]:
```

Figura 28 – Solicita um conjunto de elementos para parametrização da imagem.

```
The following acquiry parameters were provided:
Image path and filename: /home/mdelgado/MOSS/CaseStudy/PenSuspeita.E01
Case number:                Case1-MOSS
Description:                Facturas Falsas
Evidence number:            001
Examiner name:              M.Delgado
Notes:                      Pen USB 1 GB suspeita
Media type:                 removable disk
Is physical:                yes
Compression used:           best
EWF file format:            EnCase 6
Acquiry start offset:               0
Amount of bytes to acquire: 975 MiB (1022361600 bytes)
Evidence segment file size: 640 MiB (671088640 bytes)
Bytes per sector:           512
Block size:                 64 sectors
Error granularity:          64 sectors
Retries on read error:      2
Wipe sectors on read error: no

Continue acquiry with these values (yes, no) [yes]:
```

Figura 29 – Apresenta o resumo da parametrização introduzida e pede confirmação.

```
Acquiry started at: Thu Feb 23 04:59:28 2012
This could take a while.
Status: at 0%.
        acquired 32 KiB (32768 bytes) of total 975 MiB (1022361600
bytes).

Status: at 1%.
     .       .
     .       .
     .       .
Status: at 100%.
        acquired 975 MiB (1022361600 bytes) of total 975 MiB
(1022361600 bytes).
        completion in 0 second(s) with 4.8 MiB/s (5036264
bytes/second).
Acquiry completed at: Thu Feb 23 05:01:31 2012
Written: 975 MiB (1022362916 bytes) in 2 minute(s) and 03 second(s)
with 4.8 MiB/s (5036270 bytes/second).
MD5 hash calculated over data:     A845445FB5A07E677FD51C0D4B4EAB89
mdelgado@mdelgado-VirtualBox:~$
```

Figura 30 – Inicia o processo, calcula e disponibiliza o HASH.

```
mdelgado@mdelgado-VirtualBox:~$ sudo md5sum /dev/sdb
A845445FB5A07E677FD51C0D4B4EAB89  /dev/sdb
```

Figura 31 – Cálculo do HASH do conteúdo do dispositivo para confirmação.

Através destes exemplos, tendo em conta a coincidência do HASH calculado sobre o resultado dos diferentes comandos e o conteúdo do dispositivo alvo, podemos assegurar que, no que respeita ao processo de "aquisição", as ferramentas *Open Source* não evidenciam qualquer desvantagem relativamente à ferramenta proprietária de referência "EnCase Enterprise".

Sobre a fase de aquisição, pouco mais há a acrescentar. Estando garantido o acesso ao dispositivo alvo, independentemente do seu tipo, o uso das ferramentas apresentadas ou quaisquer outras, segue a mesma filosofia devendo, no entanto, ser sempre assegurada a certificação do resultado através do cálculo do respectivo HASH.

6.1.4. AVALIAÇÃO.

A hipótese "H1", formulada em 3.11.2, admie como dispensável o recurso a uma ferramenta proprietária para assegurar a realização de imagens "Bit Stream", de um dispositivo de armazenamento, no âmbito da fase de "Aquisição".

Efectivamente, a ferramenta proprietária analisada realiza a imagem em menos tempo. Contudo ao nível da segurança a ferramenta proprietária está limitada aos algoritmos MD5 e SHA1, o que não sucede com as alternativas *Open Source*. Considera-se ainda que as ferramentas *Open Source* apresentam maior versatilidade para este tipo de tarefa, tornando-se desnecessário adquirir uma ferramenta proprietária para este efeito. Confirma-se assim a hipótese n.º 1 formulada em 3.11.2.

Tabela 1 – Avaliação CENÁRIO-1-MOSS.

Ferramenta	Velocidade	Segurança	Versatilidade
EnCase	1 m e 11 s	++	++
dd	3 m e 53 s	++	++
EwfAcquire	2 m e 3 s	+++	++++

6.1.5. "CENÁRIO-2_-MOSS"- RECUPERAÇÃO DE PARTIÇÕES APAGADAS

O caso em análise envolve um disco rígido de 2GB de capacidade, cuja imagem pericial começou por revelar não existir qualquer informação acessível ao sistema operativo.

6.1.5.1.– ANÁLISE UTILIZANDO "ENCASE"

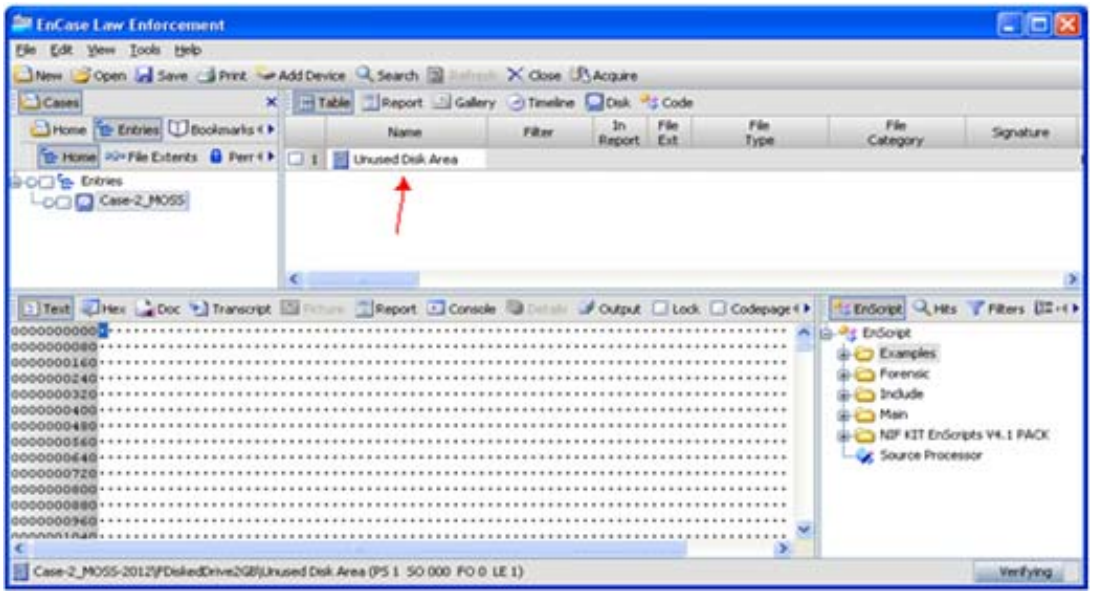

Figura 32– Plataforma EnCase Enterprise com evidence file "Case-2_MOSS" montado.

A informação assinalada, "Unused Disk Area", revela que não existe qualquer cluster atribuído. Esta situação pode indiciar a eliminação da(s) partições lógicas do dispositivo, pelo que, deverá ser investigada essa possibilidade.

Tendo em conta que o sector "0" do disco contém o Master Boot Record (MBR) e este, por sua vez, contém o código de inicialização, a tabela de partições, e a respectiva assinatura, vamos analisar o conteúdo desse sector.

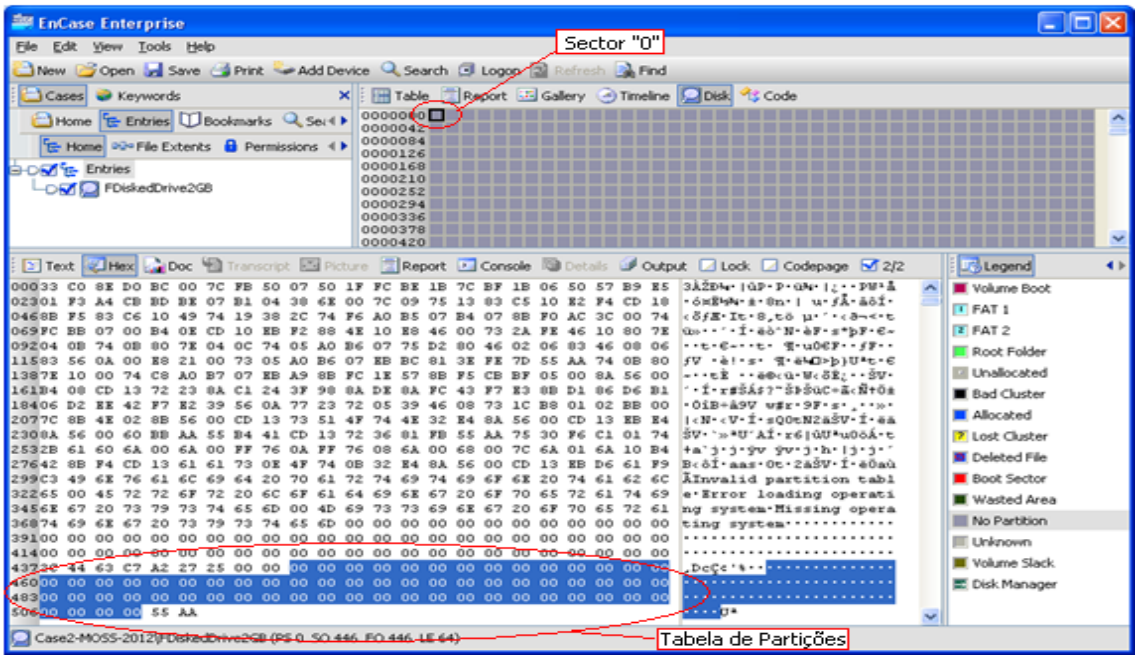

Figura 33 – Evidence file "Case-2_MOSS" vista do Sector "0"do disco físico.

Recorrendo à ferramenta "Disk View", vamos visualizar o conteúdo do primeiro sector (Fig. 28). O facto de existir informação neste sector confirma que não foi feito o Wipe ao disco (Hughes e Coughlin, 2002), abrindo perspectivas para a recuperação da partição. De acordo com as especificações do MBR, (Landis, 2002), a tabela de partições é descrita pelos 64 bytes ente o offset 446 e 509.

A figura anterior, evidencia os referidos 64 bytes preenchidos com zeros, o que confirma que as partições foram efectivamente removidas.

De acordo com a geometria do disco (Koehler, 2005), cada pista tem 63 sectores e o Volume Boot Record (VBR) da primeira partição está no primeiro sector da segunda pista, que corresponde ao sector 63. Ao visualizar o conteúdo do sector 63, (Fig. 29), confirma-se a existência de uma partição NTFS, que o EnCase nos permite montar

imediatamente, activando o menu de contexto com o botão direito do rato e escolhendo a opção "Add Partition".

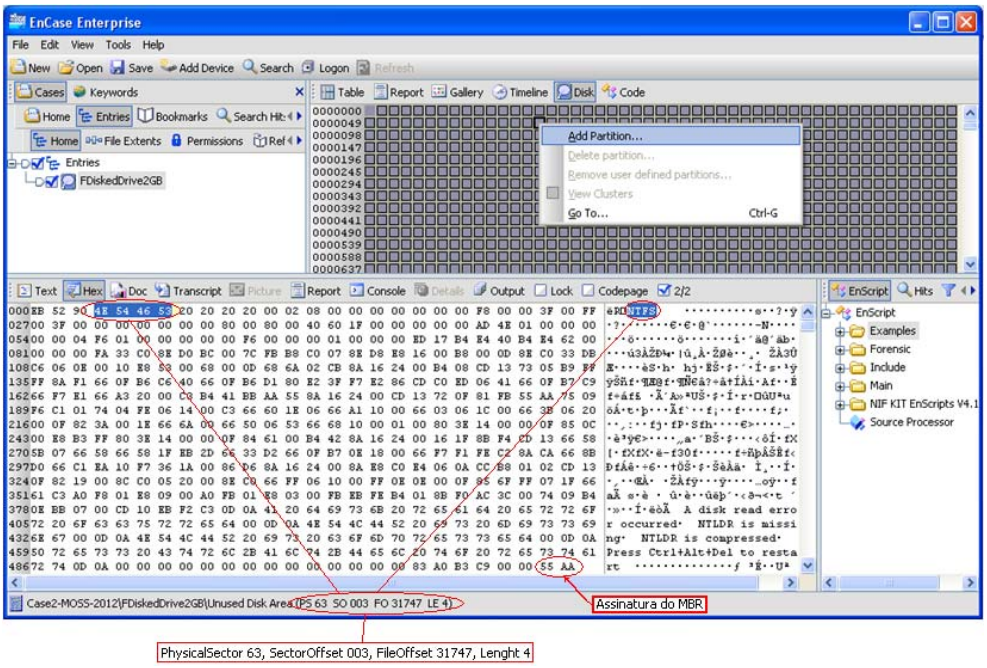

Figura 34 – Identificar VBR (sector 63).

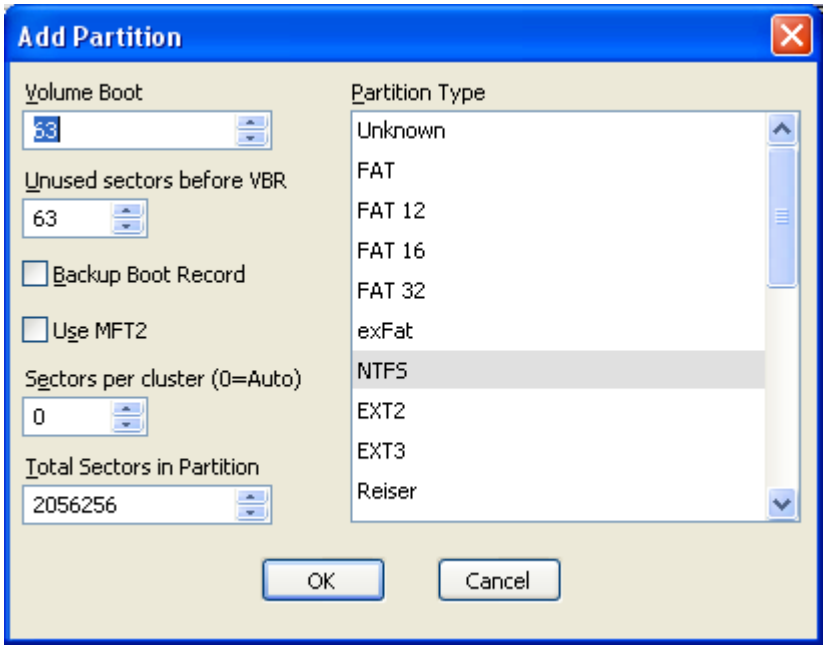

Figura 35 – Montagem da partição.

Em alternativa a este método, caso o sector 63 não evidenciasse informação, ter-se-ia que recorrer ao script "Case Processor", disponível no separador "EnScript", para pesquisar identificadores das partições, o que tornaria muito mais demorado o processo.

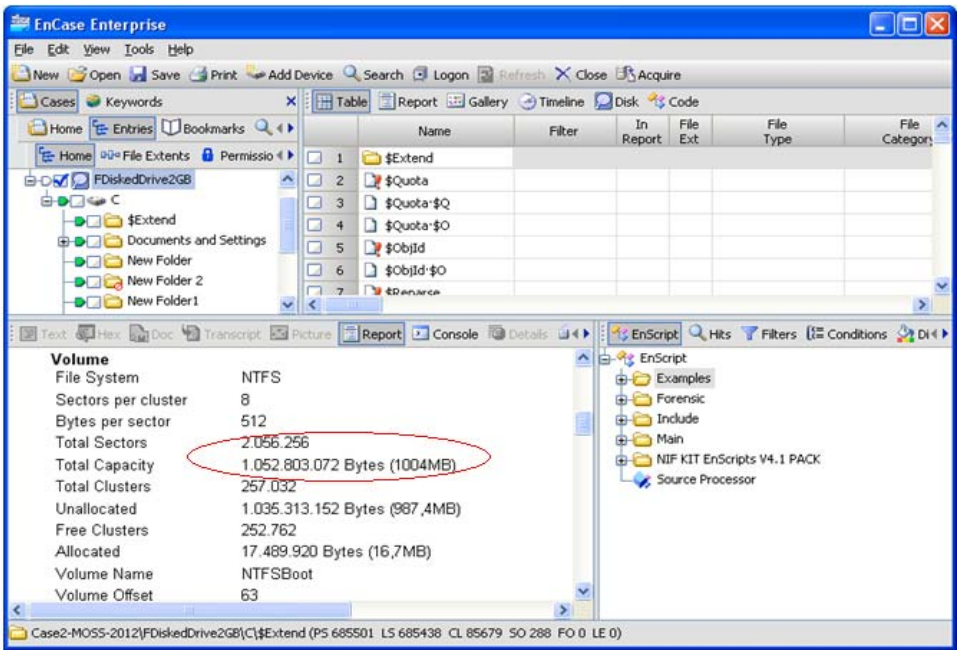

Figura 36 – Partição montada possibilitando a análise do respectivo conteúdo.

Verifica-se contudo, que a partição montada apenas ocupa 2.056.256 sectores do disco, perfazendo um total de pouco mais de 1 GB. Sendo a capacidade do disco de 2GB, é possível que, na parte restante, se possam encontrar outras partições.

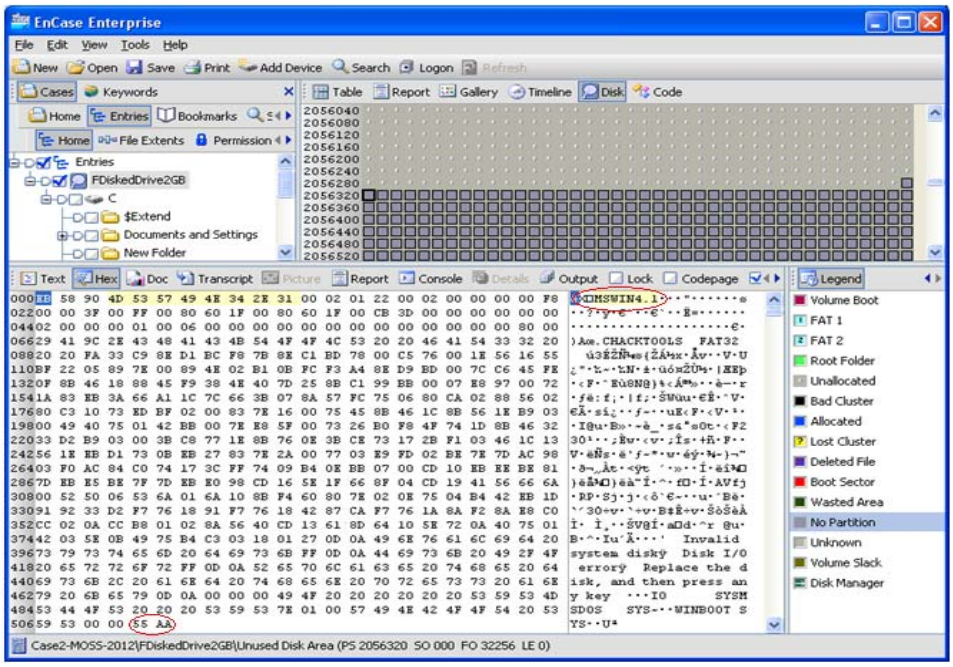

Figura 37 – Análise do conteúdo do sector 2.056.320 revela nova partição.

Uma forma de avaliar pode passar por investigar os sectores que se localizam na vizinhança dos limites desta partição, ou seja a partir do sector: 2.056.319 = (2.056.256 + 63).

Efectivamente, ao analisar o sector 2.056.320, verifica-se a existência do identificador "MSWIN4.1" que corresponde a uma partição Windows 98 (Carrier, 2005). Ao montar mais esta partição, verificamos tratar-se de uma partição FAT32 com 988,6 MB, com o nome do volume "HACKTOOLS".

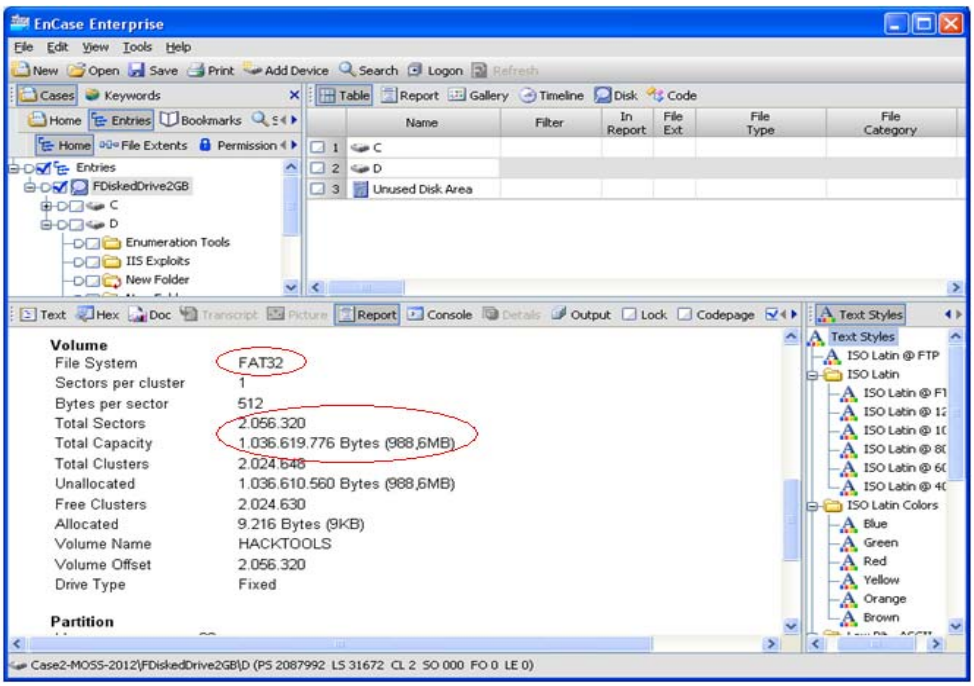

***Figura 38* –** Nova partição com 988,6 MB montada.

6.1.5.2.– ANÁLISE COM FERRAMENTA *OPEN SOURCE*

A ferramenta *Open Source* escolhida para realizar a recuperação de partições foi o TestDisk.

O TestDisk é um poderoso software *Open Source*, distribuído sob licenciamento GPL v2+, inicialmente concebido para a recuperação de partições, que possibilita igualmente a recuperação de dados em geral.

Entre as funcionalidades que o TestDisk disponibiliza contam-se:

- Correcção da tabela de partições, recuperação de partições apagadas;
- Recuperação de setores de início de partições FAT32 e respectiva cópia;
- Reconstrução de setores de início de partições FAT12/FAT16/FAT32;
- Correcção de tabelas FAT;
- Reconstrução de setores de início de partições NTFS;
- Recuperação de setores de início de partições NTFS e respectiva cópia;

- Correcção da MFT usando o mirror MFT;
- Localização do Super Bloco de backup ext2/ext3/ext4.

```
mdelgado@mdelgado-VirtualBox:/media/EnCaseTrain/MOSs$ sudo testdisk
/log Case2-MOSS.001
[sudo] password for mdelgado:
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
TestDisk exited normally.
You have to reboot for the change to take effect.
```

Figura 39 – Lançar o TestDisk na linha de comando.

O comando foi lançado com a opção que possibilita a criação de um log, o qual será reproduzido no anexo II.

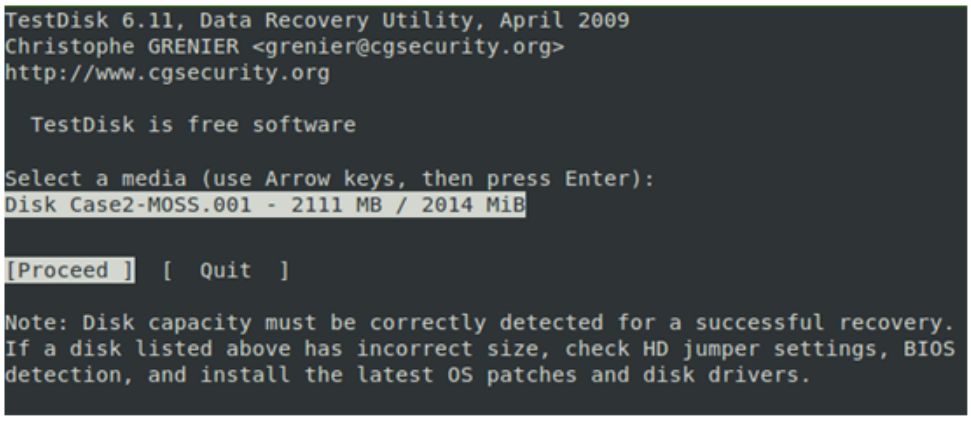

Figura 40 *– Interface do TestDisk – Seleccionar o dispositivo.*

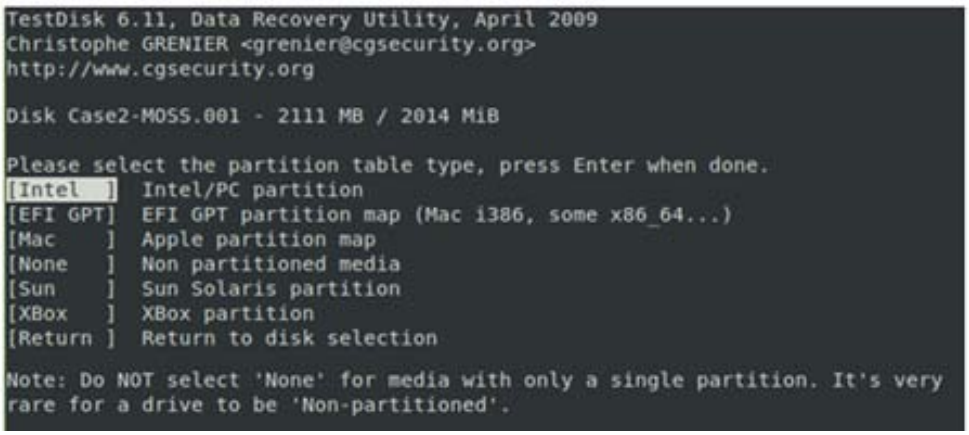

Figura 41 *– Interface do TestDisk – Seleccionar o tipo de partição.*

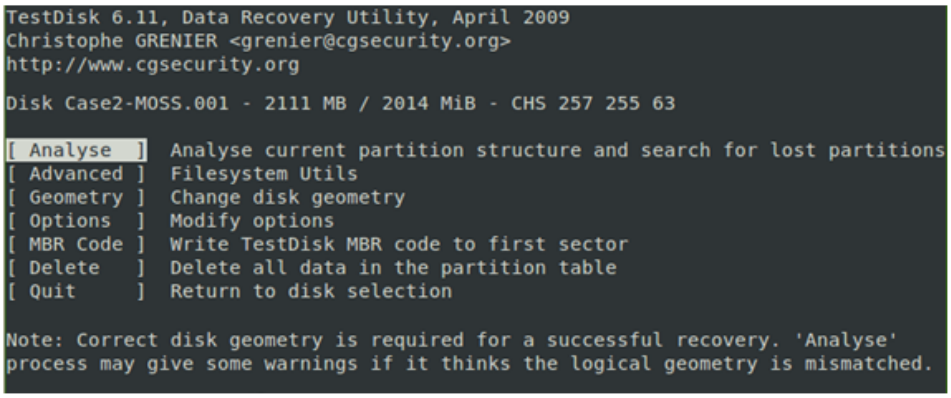

Figura 42 – *Interface do TestDisk – Seleccionar o tipo de partição.*

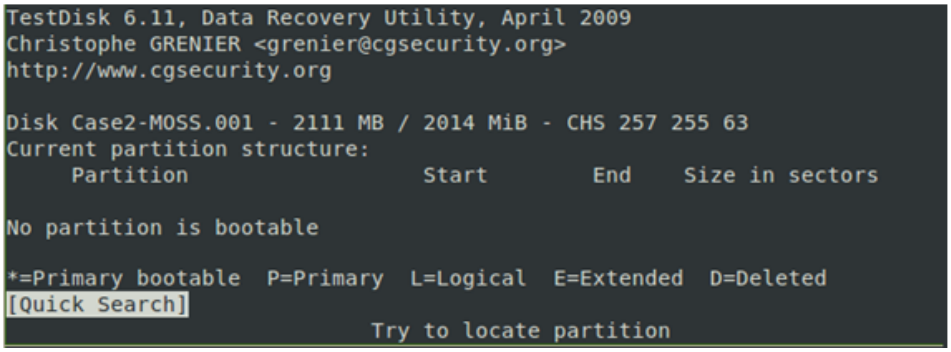

Figura 43 - *Interface do TestDisk – Não detecta partição de arranque.*

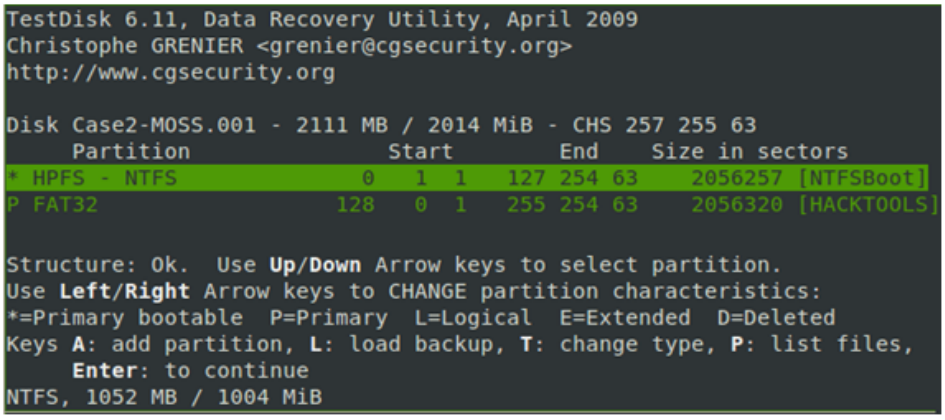

Figura 44 – *Interface do TestDisk detecta as duas Partições.*

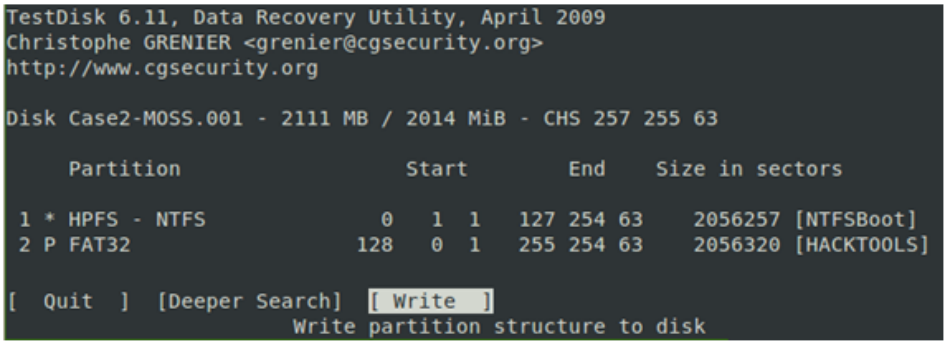

Figura 45 – *Interface do TestDisk Partições recuperadas.*

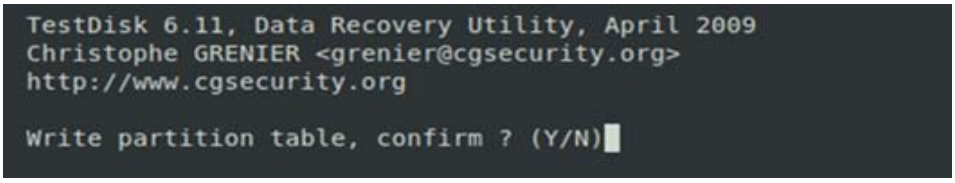

Figura 46 – *Interface do TestDisk Confirmação de gravação.*

Confirmada a gravação, toda a informação constante das duas partições passa a estar disponível, tal como sucedeu com o EnCase Enterprise.

Tabela 2 – Avaliação CENÁRIO-2-MOSS.

Ferramenta	**Velocidade**	**Precisão**	**Fiabilidade**
Proprietária	12 m e 48 s	+	+
Open Source	1 m e 3 s	++++	++++

O procedimento realizado com a ferramenta proprietária necessita da intervenção do examinador, fazendo apelo directo aos respectivos conhecimentos e deixando do lado deste parte do sucesso da acção, dado que a ferramenta não detecta por si só as partições apagadas.

Contrariamente, a ferramenta *Open Source* utilizada, detectou numa única passagem as duas partições apagadas, e assegurou a respectiva recuperação num intervalo mínimo de tempo, ganhando em tempo de execução, em precisão e em fiabilidade.

As vantagens evidenciadas pela ferramenta *Open Source*, confirmam assim a hipótese n.º 2 formulada em 4.4.3.9.

6.1.6. "CENÁRIO-3-MOSS" – PESQUISA POR PALAVRA-CHAVE

O terceiro caso tem por base a imagem do conteúdo de uma Pen USB de 16MB, na qual se irá desenvolver uma pesquisa tendo como "Palavra-Chave" o identificador de uma encomenda transportada através do operador UPS, relacionada com transacções à margem da lei.

6.1.6.1. – ANÁLISE COM ENCASE

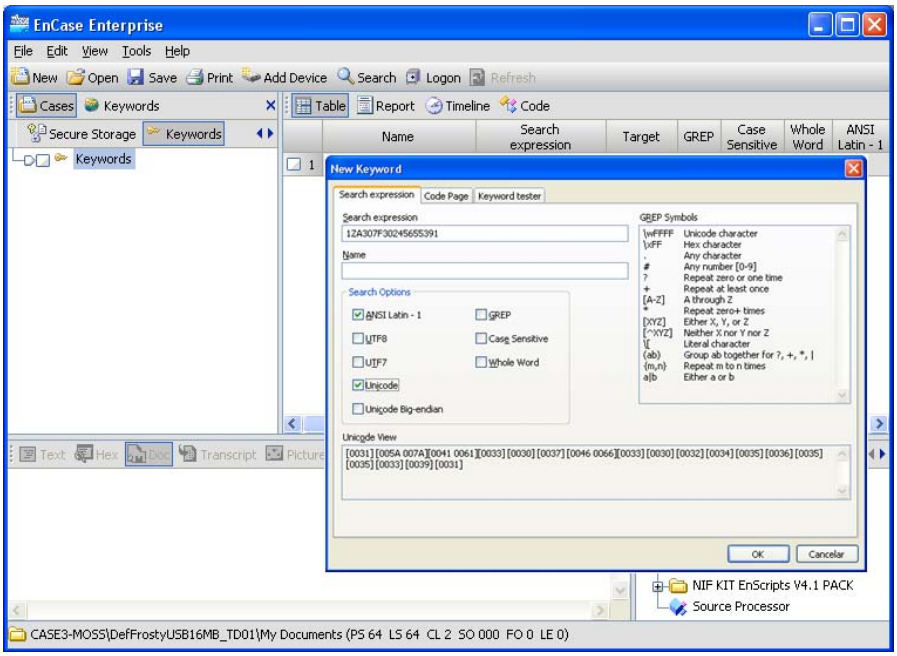

Figura 47 – Introdução da "Palavra-Chave"

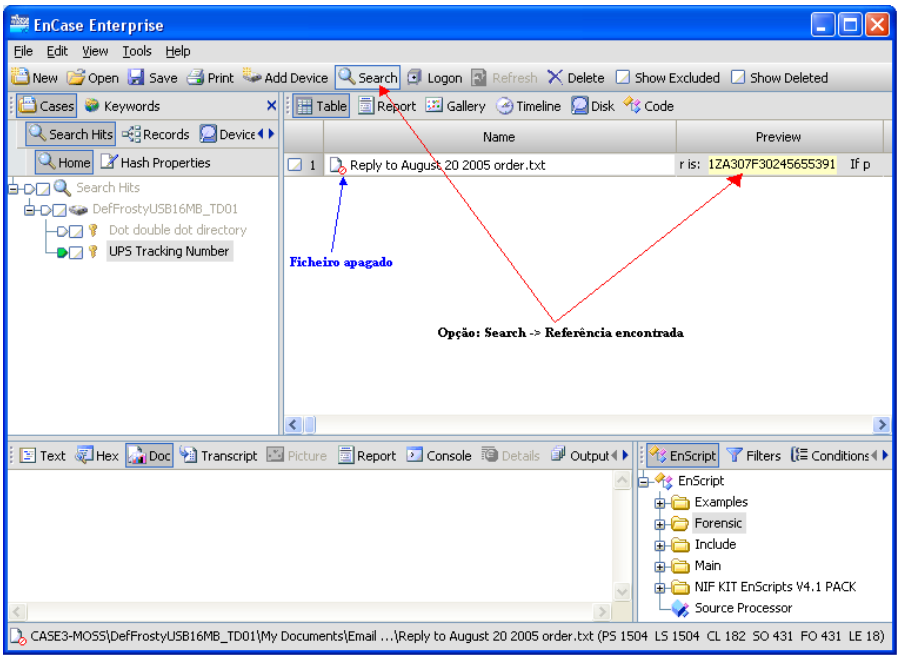

Figura 48 – Referência encontrada no ficheiro"Replay to August 20 2005 order.txt".

A palavra-chave pesquisada foi detectada no interior de um ficheiro apagado, cujo conteúdo pode ser visualizado no EnCase, fazendo o Bookmark do texto.

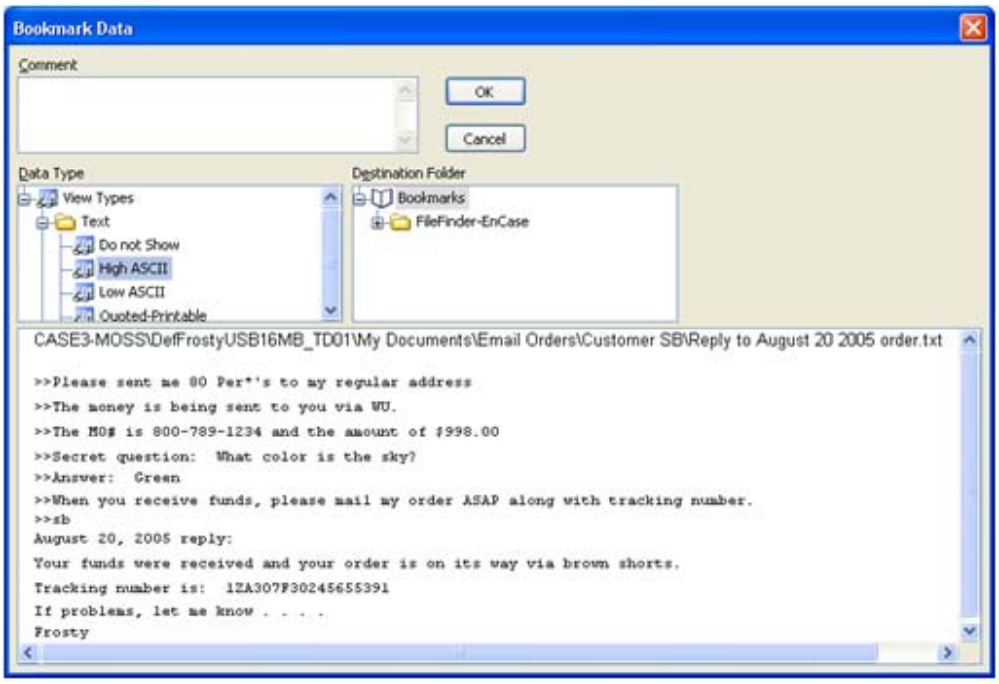

Figura 49 – Texto integral do ficheiro suspeito "Replay to August 20 2005 order.txt".

6.1.6.2.– ANÁLISE COM FERRAMENTA *OPEN SOURCE*

A ferramenta *Open Source* escolhida para realizar esta pesquisa foi o Autopsy/Sleuth Kit, descrita no anexo I da dissertação.

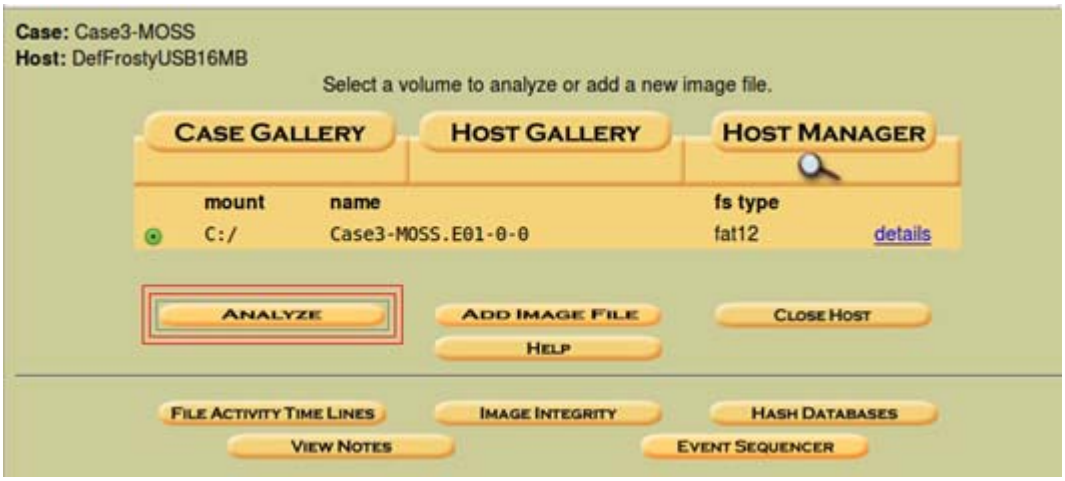

Figura 50 – Após carregar a imagem, activar opção "Análise"

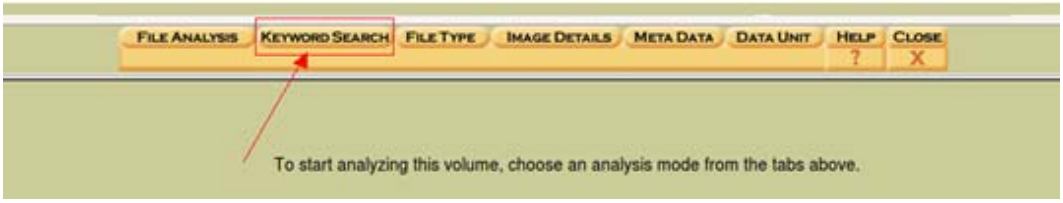

Figura 51 – Opção "KeywordSearch"

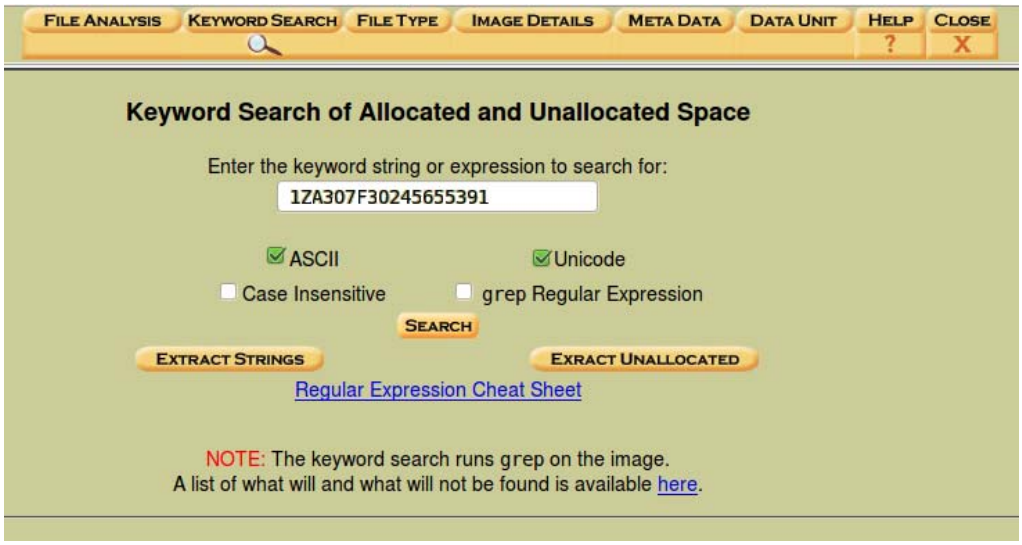

Figura 52– Introdução da "Palavra-Chave"

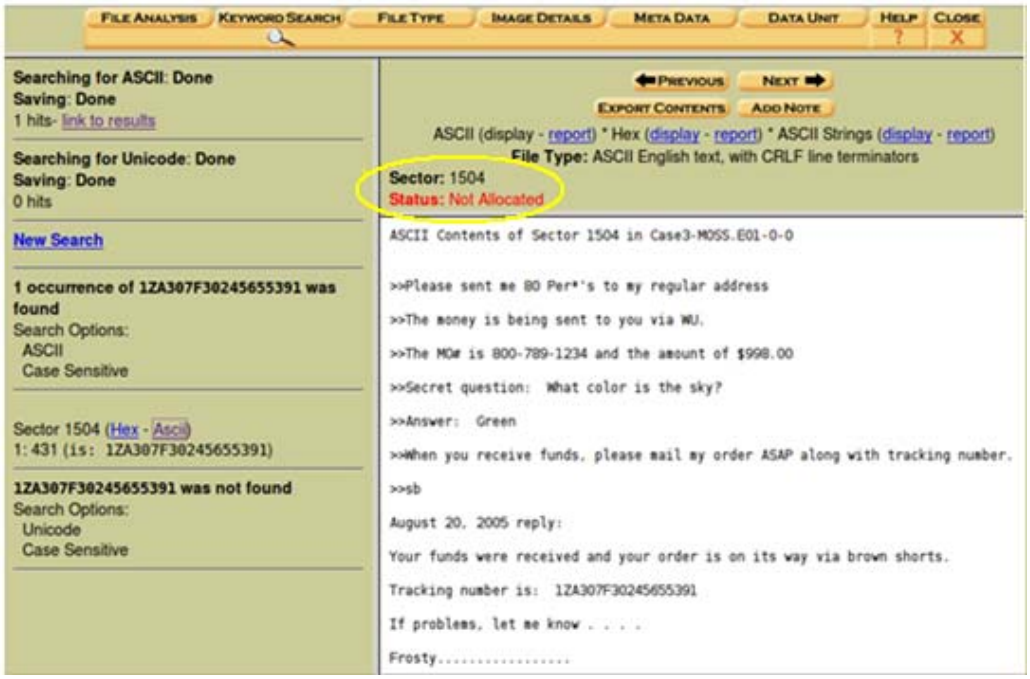

Figura 53 – Referência detectada em ficheiro localizado em espaço não alocado

Mais uma vez se demonstrou a eficiência da ferramenta *Open Source* na detecção da referência procurada, permitindo a visualização do ficheiro "hospedeiro" identificado em espaço não alocado.

Contudo, para uma avaliação mais objectiva desta funcionalidade desenvolveu-se em complemento a este estudo, uma pesquisa com 10 Palavras-Chave sobre a imagem do disco utilizado no CENÁRIO- 4 "Case-4-MOSS", com cada uma destas ferramentas.

No EnCase, o funcionamento da ferramenta “Keyword Search” é extremamente versátil e funcional permitindo introduzir todo o conjunto de palavras-chave de uma só vez e desencadear o processo de pesquisa, que se desenvolve de forma automática da primeira à última palavra.

Já o Autopsy, apenas admite pesquisa palavra a palavra, tornando o processo extremamente moroso e desconfortável.

Os resultados obtidos em cada uma das ferramentas, estão resumidos na tabela 3.

Tabela 3 – Resultados KeyWord Search.

	EnCase Enterprise	Sleuth Kit Autopsy
Bank	48	39
Check	111	80
invoice	0	0
Dollars	0	0
withdraw	0	0
hotmail	800	698
passport	45	38
crack	476	326
hacking	642	367
password	959	502

Esta síntese dos resultados devolvidos por cada uma das ferramentas evidencia um claro desequilíbrio a favor da ferramenta proprietária. Os outputs respeitantes a esta análise, dado o elevado número de páginas, serão apenas incluídos no CD-ROM entregue conjuntamente com a presente dissertação.

Efectivamente, a ferramenta Autopsy-SleuthKit, revela claras insuficiências, que resultam do facto desta não incluir propriamente uma ferramenta para pesquisa por palavra-chave, mas fornecer apenas uma interface para o comando 'grep' existente na maioria das distribuições Linux/Unix.

Para realizar uma pesquisa por palavra-chave, o SleuthKit executa em primeiro lugar o comando "strings" sobre o arquivo de imagem do sistema, executando de seguida o comando "grep" sobre os resultados do comando 'strings'. Deste modo, o sistema de

ficheiros é integralmente examinado, incluindo estruturas de meta-dados, espaço alocado, espaço não alocado, e espaço slack, em busca da palavra-chave.

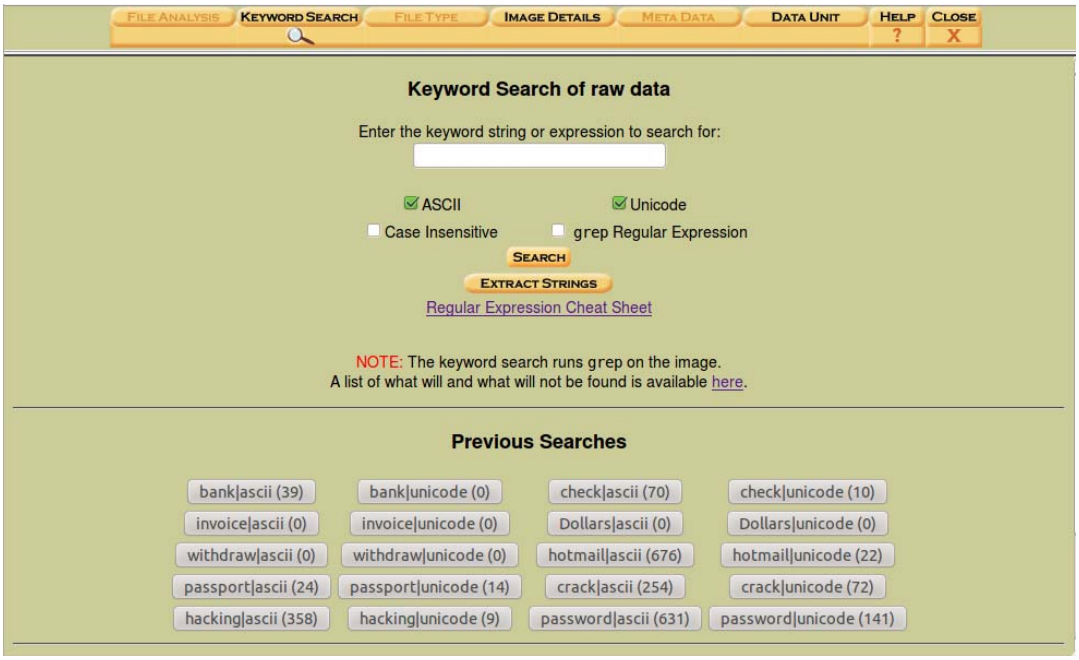

Figura 54 – Resultado final "Keyword Search"

Recorrendo ao uso de uma combinação dos comandos 'dcalc', 'ifind', e 'ffind', a pesquisa devolve o nome do ficheiro, meta-dados, ou o número dos clusters que contêm a palavra-chave.

Dado que o comando 'grep' ignora as estruturas do sistema de ficheiros, identificará qualquer ocorrência mesmo que a string pesquisada atravesse zonas de fronteira, podendo ocorrer a detecção de falsos-positivos em situações do tipo: uma parte da cadeia a pesquisar, encontra-se no final de um ficheiro, estendendo-se para o início do ficheiro seguinte;

Inversamente, nas situações em que o ficheiro se encontra fragmentado, o grep não é capaz de detectar a sequência quando esta se estende por vários fragmentos, embora a referida sequência exista perfeitamente clara e completa dentro do ficheiro quando este se encontra aberto.

As insuficiências denotadas por esta funcionalidade disponibilizada pelo Autopsy, justificam as discrepâncias que a tabela dos resultados obtidos no teste evidencia.

Dada a importância deste tipo de funcionalidade para a generalidade dos processos de investigação, o desenvolvimento de uma ferramenta vocacionada para a pesquisa por

palavra-chave, constitui uma prioridade no processo de optimização da suite Sleuth Kit Autopsy.

Tabela 4 – Avaliação CENÁRIO-3-MOSS.

Ferramenta	Velocidade	Precisão	Fiabilidade
Proprietária	2 m e 8 s	+++	+++
Open Source	53 m e 13 s	+	+

Efectivamente, as insuficiências evidenciadas pela ferramenta *Open Source*, face ao desempenho da ferramenta proprietária, coloca-a bastante longe do nível desejável, confirmando-se a hipótese 3 formulada em 4.4.3.9.

6.1.7. "CENÁRIO-4-MOSS" – RECUPERAÇÃO DE FICHEIROS EM ESPAÇO NÃO ATRIBUÍDO

O quarto caso tem em vista a recuperação extensiva de ficheiros existentes no espaço não atribuído (unallocated) de um disco. Para tal vamos utilizar a imagem de uma PenDrive de 1GB.

6.1.7.1. ANÁLISE UTILIZANDO "ENCASE"

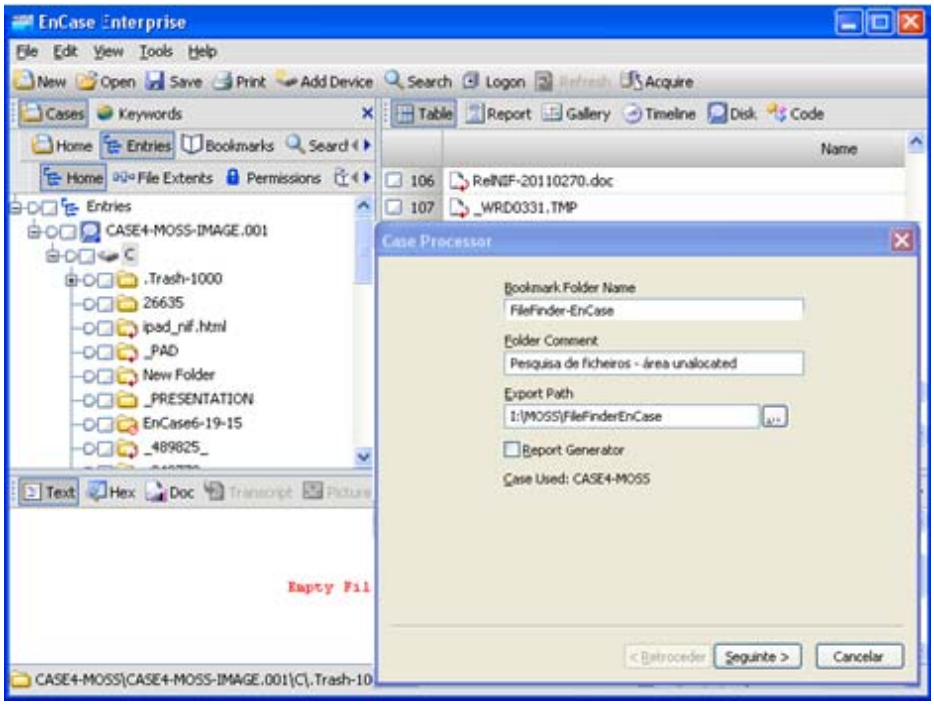

Figura 55 – Pesquisar área Unallocated com Case Processor EnCase

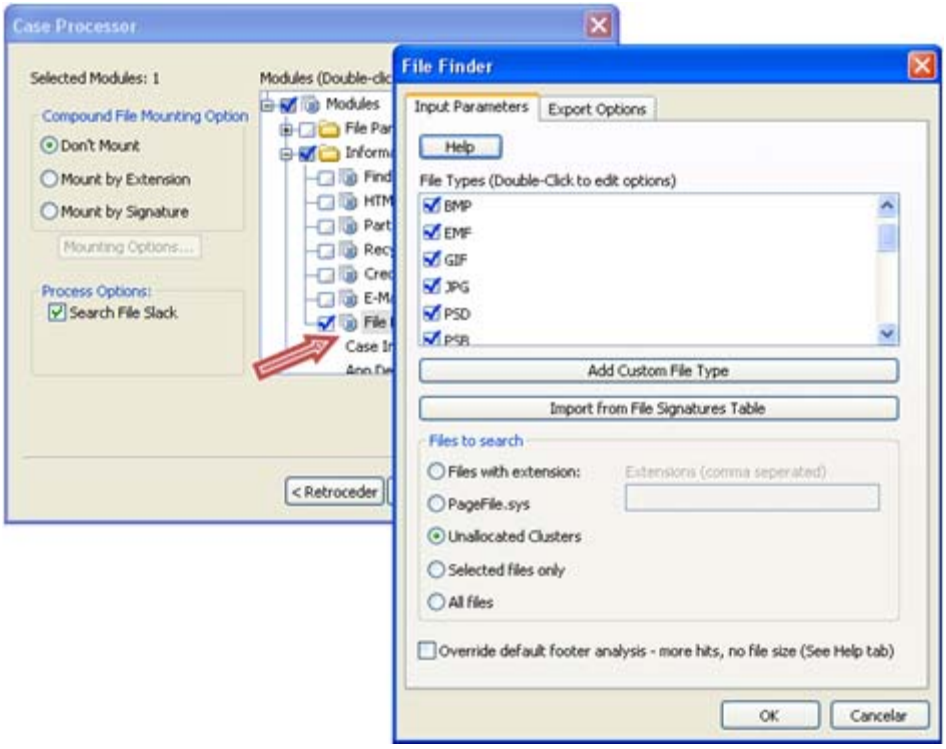

Figura 56 – Parametrização da pesquisa com EnCase

A parametrização envolveu a totalidade dos tipos de ficheiros admitidos pelo EmCase.

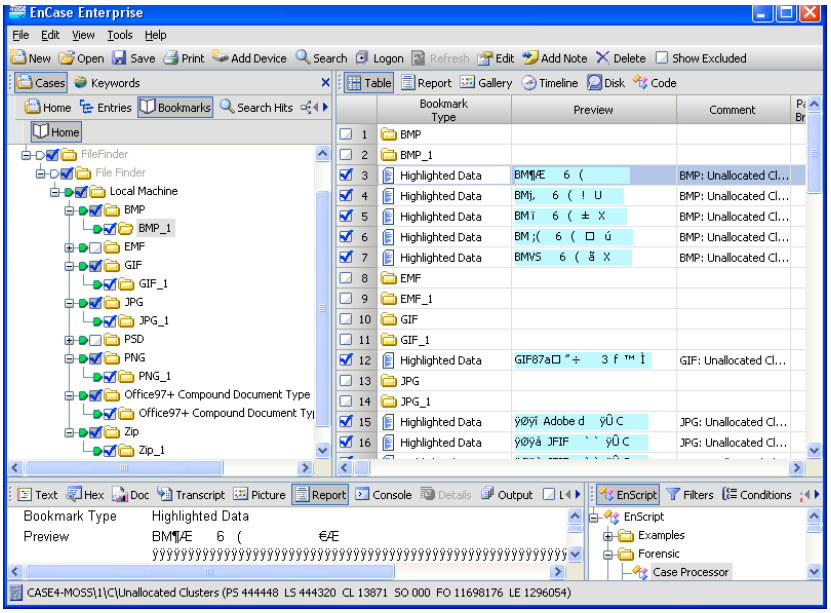

Figura 57 – Resultado da pesquisa com EnCase

O resultado da pesquisa efectuada através do EnCase, cujo relatório, dado o elevado número de páginas, será integrado no CD-ROM, traduziu-se na recuperação de um total de 50 ficheiros.

6.1.7.2. ANÁLISE COM FERRAMENTA *OPEN SOURCE*

A ferramenta *Open Source* escolhida para realizar a recuperação de ficheiros a partir de espaço não alocado, foi o PhotoRec.

O PhotoRec é um software *Open Source* multi-plataforma distribuído conjuntamente com o TestDisk sob "GNU General Public License (GPLV v2 +)", concebido para recuperar ficheiros perdidos, nomeadamente imagens, em diversos tipos de suportes. Dado que este software ignora o sistema de ficheiros do dispositivo alvo, preocupando-se apenas com a informação subjacente, o seu funcionamento não é condicionado, mesmo que o sistema de ficheiros dos suportes alvo se encontre danificado ou tenha sido reformatado.

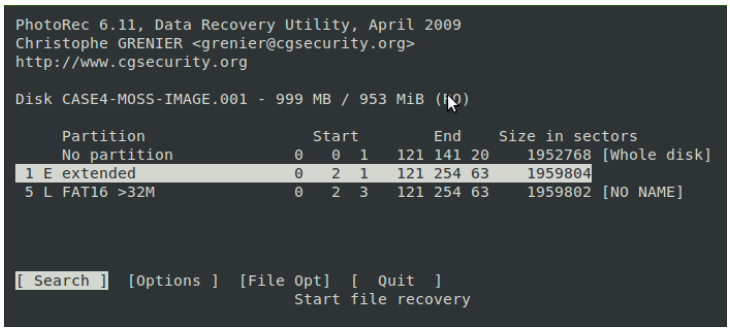

Figura 58 – PhotoRec - Selecção da partição.

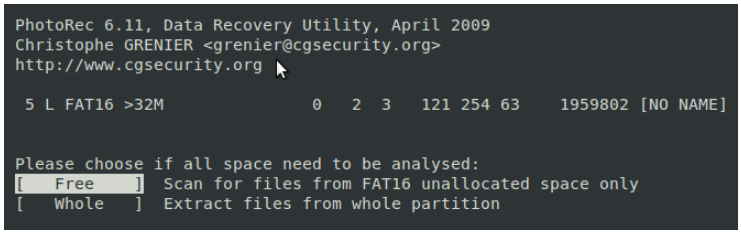

Figura 59– PhotoRec – Opção pesquisar apenas Unallocated space.

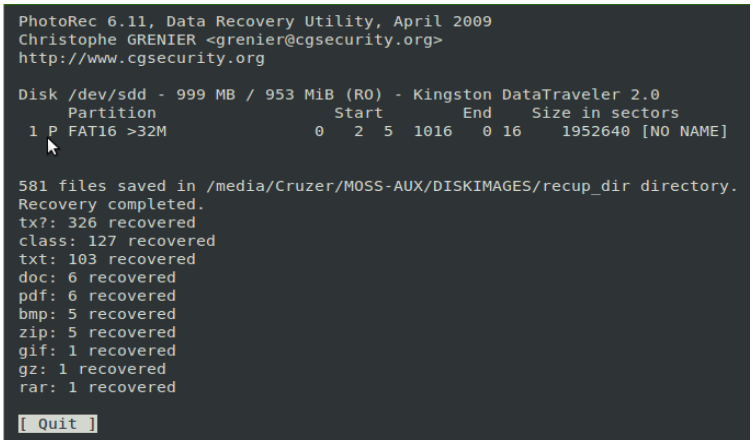

Figura 60 – Resultado da pesquisa com PhotoRec.

O resultado da pesquisa efectuada através do PhotoRec, cujo detalhe consta do respectivo ficheiro de log, disponível no CD-ROM, traduziu-se na recuperação de um total de 581 ficheiros.

Quando se pretende a recuperação do maior número possível de provas, a discrepância significativa entre o número de ficheiros recuperados pela ferramenta proprietária e o produto *Open Source* aqui testado, determina que seja este último o preferido para tarefas desta natureza.

Tabela 5 – Avaliação CENÁRIO-4-MOSS.

Ferramenta	Velocidade	Precisão	Fiabilidade
Proprietária	1m e 50s	+	+
Open Source	1m e 25s	++++	++++

A maior precisão da ferramenta *Open Source* resulta da capacidade de reconhecer um maior número de tipos de ficheiros, o que, implicitamente, favorece a respectiva fiabilidade quando o que está em causa, no âmbito da investigação, é precisamente "não deixar nenhum indício por explorar".

As vantagens evidenciadas pela ferramenta *Open Source*, confirmam assim a hipótese n.º 4 formulada em 4.4.3.9.

6.1.8. CENÁRIO-5-MOSS – PESQUISA NO "REGISTRY"

O quinto e último caso tem por objectivo a recolha de elementos a partir do "registry" do Windows, que permitam confirmar a utilização de um dado dispositivo de armazenamento, num determinado sistema.

Os dispositivos "USB" são utilizados principalmente para o armazenamento de dados simples. Contudo, a sua capacidade tem vindo a aumentar significativamente, podendo comportar quantidades apreciáveis de dados. Ao nível da investigação, a par da identificação de dados relevantes existentes nesses dispositivos, interessa igualmente determinar como esses dados ali chegaram e quem os ali colocou.

Num disco rígido do computador, estas questões encontram resposta na análise das contas de utilizador e outros artefactos do sistema operacional. No que respeita aos dispositivos "USB" levantam-se as seguintes questões:

1.º- Existem evidências no disco rígido que permitam confirmar que um utilizador do sistema fez uso de uma unidade portátil de armazenamento?

2.º - É possível encontrar evidências que permitam identificar quem usou esse dispositivo no sistema?

3.º - É possível encontrar evidências que permitam perceber em que outros sistemas da rede local o dispositivo possa ter sido ligado?

Efectivamente, um dos cenários com que nos podemos confrontar é, perante um dispositivo "USB" suspeito, ter que determinar a extensão da respectiva utilização, bem como, identificar o(s) utilizador(es) envolvido(s).

A maioria dos dispositivos USB, tem um conjunto de propriedades armazenadas no seu firmware, que permitem a respectiva identificação por parte do sistema operativo, de modo a que este possa carregar os controladores de dispositivo apropriados, permitindo assim a sua utilização.

Alguns dos campos de firmware presentes na maioria dos dispositivos que endereçam características físicas são:

- idVendor: um número atribuído para identificar o fornecedor, por exemplo: IE "1307" identifica: USBest Technology Inc.;
- idProduct: um número de identificação do produto - IE produto / modelo "0163";
- iManufacturer: descrição do fabricante "USBest Technology";
- iProduct: descrição do tipo de produto "USB Mass Storage Device";
- iSerialNumber: um número de série do dispositivo. Este campo pode ser muito útil na identificação de um dispositivo USB conectado a um único computador.

O utilitário UVCViewer.exe, disponibilizado pela Microsoft no âmbito do Windows Driver Kit (WDK)[5], permite aceder a essa informação.

Destaca-se ainda, ao nível lógico, outro item relevante que consiste na identificação do número de série do volume.

Numa situação real, podemos ou não ter em mãos uma Flash Drive da qual procuramos evidências num sistema. Em alguns casos, tudo o que temos é a suspeita de que alguém usou uma flash drive USB num dado sistema. Suspeita essa, que somos convidados a confirmar.

No caso presente, temos uma Flash Drive, com a referência "SanDisk", apreendida por suspeita de ter sido utilizada para copiar ficheiros importantes, entretanto removidos do sistema onde se encontravam. Pretendemos confirmar se ela foi efectivamente usada nesse sistema e em que data(s), através da análise do "registry" do sistema.

A análise de uma situação deste tipo inicia-se com a prévia recolha dos identificadores chave do dispositivo suspeito, para posteriormente poder identificar a sua utilização nos sistemas alvo.

6.1.8.1. - LEITURA DO FIRMWARE

Com base no utilitário UVCView.exe, procedemos à recolha das características da Pen Drive Suspeita, cujo output consta do anexo III.

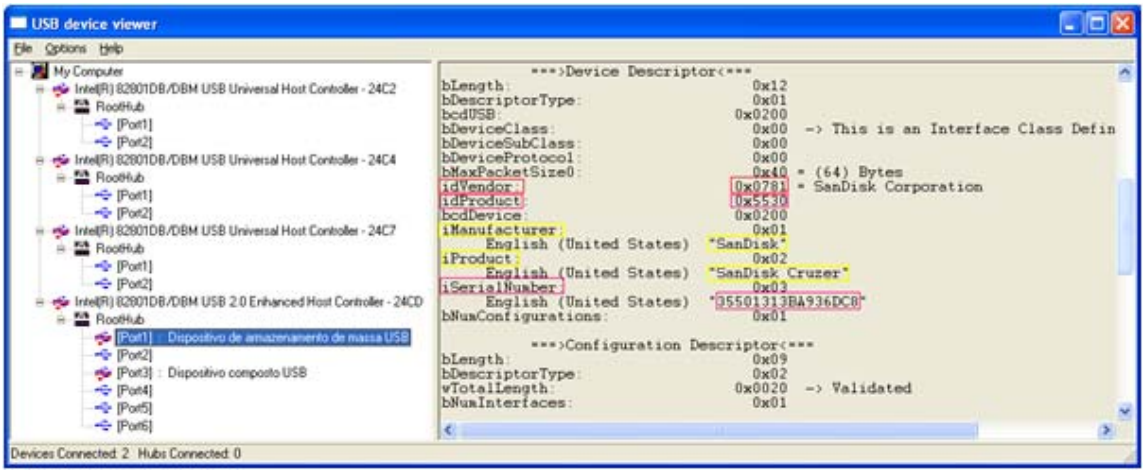

Figura 61 – Output do utilitário para visualização do firmware "UVCView.exe"

[5] http://www.microsoft.com/whdc/DevTools/WDK/WDKpkg.mspx

Os campos: idVendor e idProduct são utilizados pelo Windows para criar o identificador de instância de dispositivo na chave: HKLM/SYSTEM/Enum/USB;

Os campos: iManufacturer e iProduct são frequentemente utilizados para criar o identificador de instância do dispositivo na chave HKLM/SYSTEM/Enum/USBSTOR;

O campo: iSerialNumber é utilizado para criar um identificador exclusivo para a unidade "USB", na chave USB e faz parte da identificação de instância única na chave USBSTOR.

De posse destes elementos, nomeadamente do número de Série que identifica de forma unívoca o dispositivo USB, podemos iniciar um processo de pesquisa nos sistemas aos quais se admite que a unidade suspeita esteve ligada, de modo a identificar pistas que confirmem essa suspeita e permitam saber em que data tal se verificou.

Locais onde poderemos encontrar evidencias retidas pelo Windows XP pela passagem de uma unidade USB:

- HKLM\System (Chave de registry SYSTEM);
- HKCU (Chave de registry no ficheiro NTUSER.dat);
- Setupapi.log;
- *.LNK, Ficheiros de Link;
- Restore Points;
- Ficheiros de LOG ($logfile);
- Área de Swap (pagefile);
- Espaço não atribuído (unallocated);
- Ficheiros Prefetch.

No caso presente, a análise vai-se confinar ao “Registry”, dispondo-se, para o efeito, dos ficheiros de registry do sistema alvo.

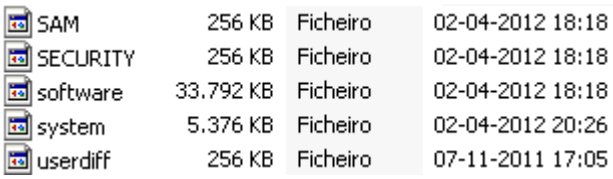

Figura 62 – Ficheiros de Registry para análise.

Para confirmar simplesmente se o dispositivo suspeito foi alguma vez conectado ao sistema e, em caso afirmativo, em que data, bastará analisar as chaves USB e USBSTOR existentes no ficheiro “System”.

6.1.8.2. ANÁLISE UTILIZANDO “ENCASE”

O Encase permite montar os ficheiros de registry, navegar na respectiva estrutura e visualizar o conteúdo das chaves, subchaves e valores. Com base nos identificadores do dispositivo USB, Vendor_id, Product_id e número de série, colhidos previamente, torna-se fácil identificar nas chaves de registry as entradas respeitantes à unidade suspeita.

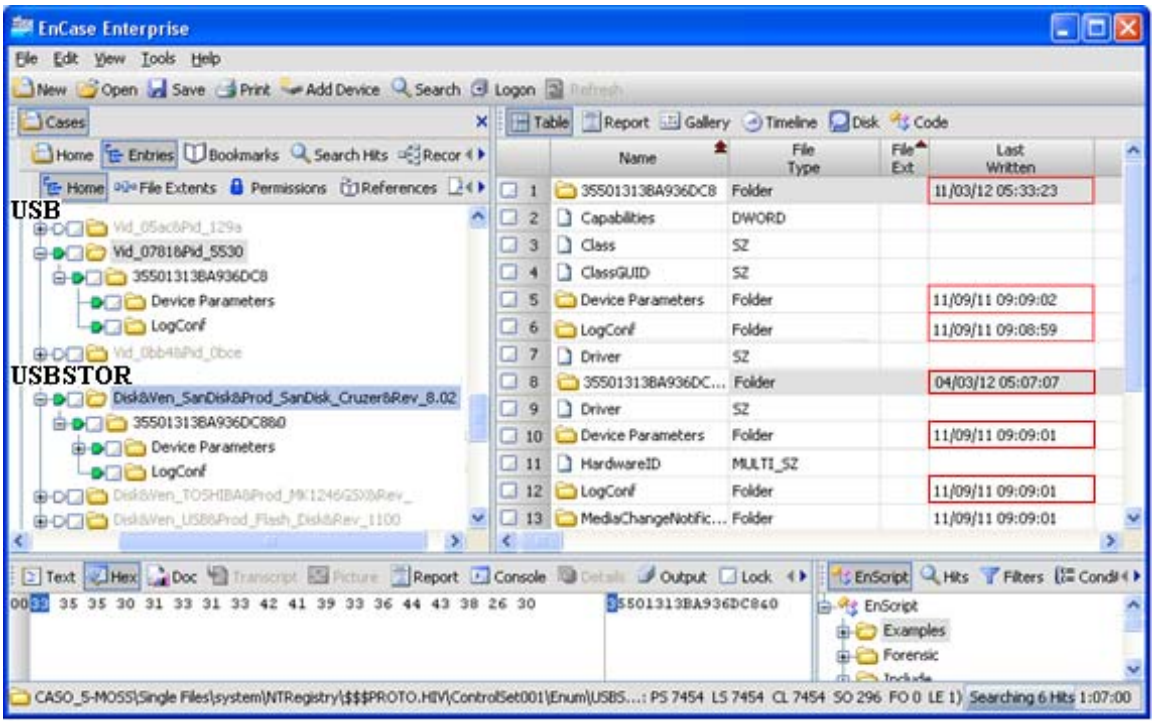

Figura 63 – Evidências que confirmam a presença da unidade suspeita no sistema.

A data da última escrita da subchave associada ao identificador único do dispositivo, número de série: “35501313BA936DC8”, corresponde à primeira vez que o dispositivo foi inserido, após uma reinicialização do sistema. Esta data mantém-se, mesmo que o dispositivo seja inserido diversas vezes, desde que não se verifiquem “reboots”, registando nova data apenas na primeira inserção após um “reboot”. Neste caso, podemos constatar que isso aconteceu no dia 3 de Abril de 2012.

Name	File Type	File Ext	Last Written
Vid_0781&Pid_5530	Folder		11/09/11 09:08:59

Figura 64 – Chave criada em HKLM/SYSTEM/Enum/USB.

A data associada à chave "Vid_0781&Pid_5530" e subchave "LogConf", corresponde ao momento em que o dispositivo foi inserido no sistema pela primeira vez, o que neste caso aconteceu no dia 9 de Novembro de 2011, às 9h:8m:59s.

6.1.8.3. ANÁLISE COM FERRAMENTA *OPEN SOURCE*

A ferramenta *Open Source* escolhida para realizar a análise do "registry" foi o RegRipper[6]. Esta ferramenta, desenvolvida e mantida por Harlan Carvey, é uma ferramenta *open source* escrita em Perl que, de uma forma bastante intuitiva e rápida, disponibiliza a informação extraída dos ficheiros específicos do registry, devidamente correlacionada, para facilitar o processo de investigação.

O RegRipper disponibiliza um vasto conjunto de plugins concebidos para tratamento específico de diversas chaves de registry, conforme detalhes constantes do anexo I.

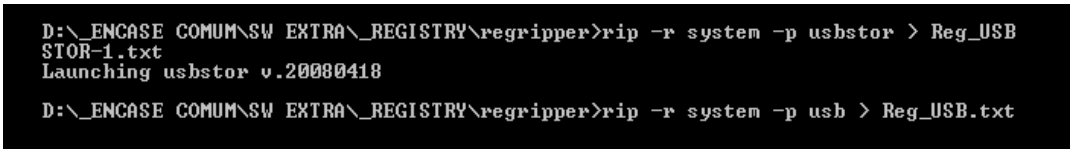

Figura 65 – Comandos para fazer o parsing das chaves USB e USBSTOR.

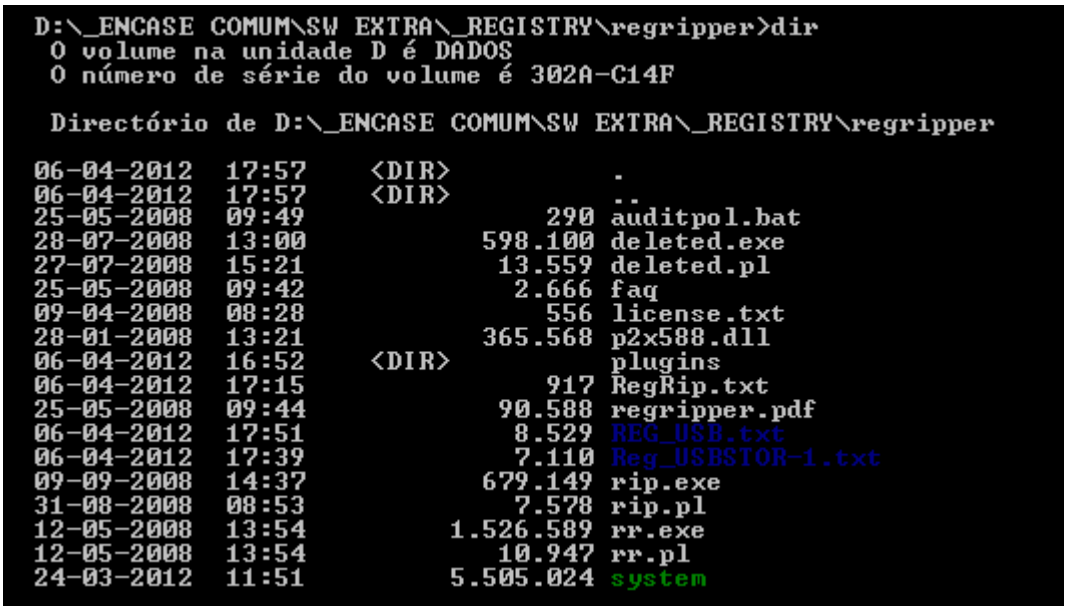

Figura 66 – Ficheiro de registry "system" e output dos dois comandos "rip".

Para validar a utilização do dispositivo suspeito neste sistema, bastará pesquisar a existência do respectivo identificador único nos ficheiros resultantes do "parsing".

[6] http://regripper.wordpress.com/regripper/

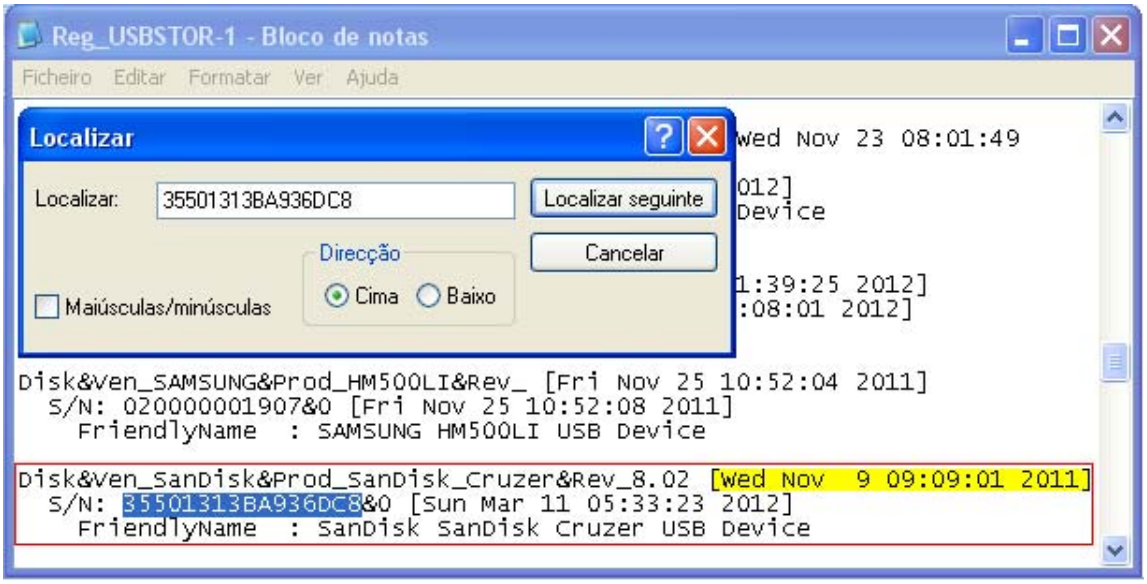

Figura 67 – Pesquisa do n.º de série do dispositivo suspeito no ficheiro Reg_USBSTOR-1.txt.

Confirma-se que o dispositivo suspeito foi efectivamente ligado ao sistema a que pertence o ficheiro de registry analisado, tendo sido conectado pela primeira vez no dia 9 de Novembro de 2011, confirmando o resultado obtido com a ferramenta proprietária.

Tabela 6 – Avaliação CENÁRIO-5-MOSS.

Ferramenta	**Velocidade**	**Precisão**	**Fiabilidade**
Proprietária	3 min e 25 s	+++	+++
Open Source	45 s	+++	+++

A ferramenta proprietária começa por montar integralmente o ficheiro de registry que pretendemos analisar, permitindo de seguida que naveguemos na sua estrutura, o que consome algum tempo. A ferramenta *Open Source*, graças aos inúmeros plugins disponíveis, permite exportar directamente para um ficheiro, o conteúdo da(s) chave(s) que pretendemos analisar, possibilitando a realização da tarefa de forma mais imediata mantendo-se idêntica precisão e fiabilidade.

Tabela 7 – Avaliação de Hipóteses: Síntese.

	HIPÓTESE	AVALIAÇÃO
H-1	Existem ferramentas Open Source que permitem obter resultados, iguais aos obtidos pelas ferramentas proprietárias, na realização de imagens "Bit Stream" de um dispositivo de armazenamento.	VALIDADA
H-2	Na investigação forense, no campo digital, as ferramentas Open Source permitem obter melhores resultados na detecção e recuperação de volumes lógicos (partições).	VALIDADA
H-3	No que respeita a ferramentas para "pesquisa por palavra-chave", as ferramentas Open Source disponíveis não estão ainda ao mesmo nível das ferramentas proprietárias.	VALIDADA
H-4	As ferramentas Open Source permitem a recuperação de ficheiros existentes nos espaços não atribuídos das unidades de armazenamento de forma mais eficaz do que as ferramentas proprietárias.	VALIDADA
H-5	Analisar o "registry" do Windows com ferramentas Open Source é possível e fornece resultados tão fiáveis como os obtidos com ferramentas proprietárias.	VALIDADA

Do trabalho empírico realizado resulta a validação da totalidade das hipóteses formuladas, (tabela 7), ficando assim demonstrada a eficácia das ferramentas *open source* no processo de investigação de casos reais de práticas criminais de natureza económica.

7. CONCLUSÕES E TRABALHOS FUTUROS

A presente dissertação apresentou como objectivo geral demonstrar a valia de um conjunto de ferramentas *Open Source* na realização de determinadas tarefas de apoio à investigação de crimes de natureza económica, tomando por referencial uma das ferramentas proprietárias de utilização mais difundida na comunidade.

Ao longo do trabalho de investigação, foram evidenciados os benefícios extremos que a investigação criminal pode retirar da Informática Forense, quando a "cena do crime" envolve equipamentos informáticos, o que, actualmente, constitui a situação mais comum.

Através do tratamento de cinco situações diferentes, todas elas frequentes em processos de investigação de crimes de natureza económica, ficou demonstrada a eficácia de um conjunto de ferramentas *Open Source*, pois, não só permitiram obter resultados idênticos aos fornecidos pela ferramenta de referência, como, em parte dos casos, os suplantou.

Muitas outras ferramentas *Open Source*, algumas das quais referenciadas no anexo I, oferecem, nesta área, performances semelhantes no tratamento de várias outras fontes de evidências digitais relevantes na investigação do crime económico. Contudo, o escasso tempo e limitado número de páginas a que a natureza deste trabalho vincula, não o permitiu aqui demonstrar. Considero, no entanto, que o objectivo traçado de deixar testemunho desta realidade, foi cumprido.

Para além do objectivo geral, foram formadas na proposta para esta dissertação, dois objectivos secundários:

1. Despertar o interesse da comunidade *Open Source* nacional para o potencial que a Computação Forense encerra, em termos de necessidades de desenvolvimento de novas ferramentas.

e

2. Despertar o interesse da comunidade académica para a necessidade de avaliar a Computação Forense, como uma área a contemplar futuramente quer em cursos do ramo tecnológico, quer nas áreas de economia, gestão e de direito.

O limitado número de trabalhos académicos existentes sobre esta matéria contrasta com a extrema importância que a Informática Forense encerra para a área da Justiça,

unanimemente reconhecida como estruturante para a normalização da vida em sociedade, profundamente desregulada no nosso país.

O carácter demonstrativo colocado no texto, limitando, sempre que possível, a utilização de terminologia técnica, tem também o propósito de facilitar a sua leitura no sentido de "ganhar para esta causa" mais adeptos que permitam, ainda que de forma limitada, cumprir estes dois objectivos, a bem da sociedade.

Um último objectivo partilhado com os meus dilectos orientadores, foi o de, no final deste trabalho, criar um "Live-CD" que permitisse disponibilizar todo o conjunto de ferramentas aqui tratado, adicionando complementarmente algumas outras com interesse para a investigação de crimes económicos.

Porém, recentes alterações na minha vida profissional, obrigaram a adiar a concretização desse objectivo, que, no entanto, continuarei a proseguir.

Termino com as palavras de Ruibin, Yun e Gaertner (2005) que considero perfeitamente actuais face à realidade nacional:

> *A Informática forense, pela sua relação com uma das áreas científicas que mais evolui actualmente, requer especial atenção, pois tende a ter um papel cada vez mais importante no campo da investigação criminal, e o actual "estado da arte", está ainda muito longe de tirar partido do potencial da "inteligência computacional" actualmente disponível, quando comparada com outras áreas de investigação.*

A constatação formulada por estes autores, perspectiva para esta área de actividade uma ampla margem de evolução.

Com a presente dissertação, procurei deixar pistas para que, depois deste, se sigam muitos mais trabalhos sobre estas matérias e que, através deles, se possa contribuir para uma sociedade mais justa e eticamente responsável.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ACPO, 2011 – Association of Chief Police Officers – UK

Good Practice Guide for Computer-Based Electronic Evidence

Disponível em: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Acedido em 8/12/2011

Afonso, O., Gonçalves, N. (2009) "Economia não Registada em Portugal"

WORKING PAPERS No 4 / 2009 (OBEGEF – Observatório de Economia e Gestão de Fraude.

Beak, Christiaan (2011) - Introduction to File Carving

Disponível em:

http://www.mcafee.com/us/resources/white-papers/foundstone/wp-intro-to-file-carving.pdf

Acedido em: 01/02/2012

Berghel,H.;Hoelzer, D.;Sthultz, M.(2006) - Data Hiding Tactics for Windows and Unix File Systems

Disponível em: http://www.berghel.net/publications/data_hiding/data_hiding.php

Acedido em: 10/1/2012

Boddington, R., Hobbs, V., Mann, G.(2008)- "Validating digital evidence for legal argument"

Murdoch University - 6th Australian Digital Forensics Conference

Disponível em: http://researchrepository.murdoch.edu.au/1878/

Acedido em: 01/10/2011

Branco, M. (2010) "Empresas, Responsabilidade Social e Corrupção"

Working Papers Nº 6/2010 OBEGEF – Observatório de Economia e Gestão de Fraude

Brezinski, Dominique, Killalea, Tom (2002) - Guidelines for Evidence Collection and Archiving

Network Working - RFC: 3227

Disponível em: http://www.ietf.org/rfc/rfc3227.txt

Acedido em: 20/11/2011

Brown, Christopher L. T. – (2005) - Computer evidence : collection & preservation (Networking & Security)

Publicado por: CHARLES RIVER MEDIA, INC.

Carlton, Gregory H (2008) - An Evaluation of Windows-Based Computer Forensics Application Software Running on a Macintosh, Publicado no Journal of Digital Forensics, Security and Law

Disponível em: http://www.jdfsl.org/subscriptions/JDFSL-V3N3-reprint-Carlton.pdf

Acedido em: 10/11/2011

Carrey Eoghan, (2009) – "Handbook of Digital Forensics and Investigation"

Elsevier Academic Press

Carrier, B. (2002) "Defining Digital Forensic Examination and Analysis Tools".

Digital Forensic Research Workshop 2002, Syracuse

Disponível em: http://www.dfrws.org/2002/papers/Papers/Brian_carrier.pdf

Acedido em: 10/8/2011

Carrier, B. (2003) "*Open Source* Digital Forensics Tools: The Legal Argument"

Disponível em: http://www.digital-evidence.org/papers/opensrc_legal.pdf

Acedido em: 10/9/2011

Carrier, B. (2003)-A "The Sleuth Kit"

Disponível em: http://www.sleuthkit.org/sleuthkit/docs.php

Acedido em: 10/11/2011

Carrier, B. (2003)-B "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers"

Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.14.9813

Acedido em: 10/08/2011

Carrier, B. (2005) "File System Forensic Analysis"

Addison-Wesley

Carrier, B. (2006) – "Digital Investigation and Digital Forensic Basics"

Disponivel em: http://www.digital-evidence.org/di_basics.html

Acedido em 12/08/2011.

Carvey Harland. (2005) - The Windows Registry as a forensic resource.

Disponível em: http://www.sciencedirect.com/science/article/pii/S1742287605000587

Acedido em: 28/12/2011

Ewfacquire, (2011) – Projecto *Open Source*: acquires data in the EWF format

Disponível em: http://linux.die.net/man/1/ewfacquire

Acedido em:12/08/2011

Encase, (2011)

Disponível em: http://www.forensicswiki.org/wiki/Encase_image_file_format

Acedido em:12/08/2011

Farmer, D. Venema, W. (2005) – "Forensic Discovery"

Addison-Wesley Professional Computing Series

FIPS, (1995) - Federal Information Processing Standards Publication 180-1

Disponivel em: http://www.itl.nist.gov/fipspubs/fip180-1.htm

Acedido em: 1/08/2011

Friedrich Schneider, Andreas Buehn,Claudio E. Montenegro (2010)

New Estimates for the Shadow Economies all over the World International Economic Journal-Vol: 24, Issue: 4, Pg: 443-461

Disponível em: http://www.tandfonline.com/doi/abs/10.1080/10168737.2010.525974

Acedido em: 1/08/2011

Galves F.,Galves, C. (2004)- Criminal Justice Magazine Spring, Volume 19 Number 1

Disponível em: http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html

Acedido em 21/11/2011

Gantz, J. e Reinsel, D., (2011) - The Digital Universe Decade – Are You Ready? – IDC - IVIEW

Disponível em: http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm

Acedido em 1/08/2011

Giannelli, P, (1996) - Forensic Science: Chain of Custody - Criminal Law Bulletin Volume:32 Issue:5

Disponível em**:** http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=170731

Acedido em: 12/04/2012

Gorge, M., (2005) - USB & other portable storage device usage: Be aware of the risks to your corporate data in order to take pre-emptive and/or corrective action

Disponível em: http://www.sciencedirect.com/science/article/pii/S136137230570244X

Acedido em: 21/08/2011

Ghosh, A., (2004) - Guidelines for the Management of IT Evidence

Disponível em: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf

Acedido em:10/08/2011

Gutmann, P., (2001) "Data Remanence in Semiconductor Devices "

Proceedings of the 10th conference on USENIX Security Symposium Volume 10

Disponível em: http://www.cypherpunks.to/~peter/usenix01.pdf

Acedido em: 12/01/2012

Hart, Sarah V. 2004 - NIJ – National Institute of Justice – "Forensic Examination of Digital Evidence"- A Guide for Law Enforcement

Disponível em: http://www.nij.gov/pubs-sum/199408.htm

Acedido em: 09/08/2011

Hoey, A 1996 - Analysis of the Police and Criminal Evidence Act s.69 - Computer Generated Evidence, Publicado no Web Journal of Current Legal Issues associado com Blackstone Press Ltd.

Disponível em: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCUQFjAA&url=http%3A%2F%2Fwebjcli.ncl.ac.uk%2F1996%2Fissue1%2Fhoey1.rtf&ei=d5SKT6yMDeas0QXrk8HeCQ&usg=AFQjCNHjPEXIA_8aZ9X0sRZQX-Vig47HYw&sig2=mGXQPQDOKlImJ6hxN1Q0Tw

Acedido em: 12/12/2011

Hughes, Gordon and Coughlin, Tom (2002) - Secure Erase of Disk Drive Data"

Disponível em: http://cmrr.ucsd.edu/people/Hughes/CmrrSecureEraseProtocols.pdf

Acedido em: 20/1/2012

Inmon, Keith e Rudin, Norah (2001) - Principles and Practice of Criminalistics - The Profession of Forensic Science

Insa, Fredsvinda, (2006) "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study Journal of Digital Forensic Practice, 1:285–289, 2006

IOCE (2002) – International Organization on Computer Evidence

General Definitions relating to digital evidence

Disponível em : http://www.ioce.org/core.php?ID=5

Acedido em 08/12/2011

Jain A. (2001) "Corruption: A Review"

Journal of Economic Surveys Vol. 15, n.º 1 Concordia University

Kenneally, E., (2001) - *Open Source* Software As A Mechanism To Assess Reliability For Digital Evidence

Publicado no Virginia Journal of Law and Technology Association

Disponível em: http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html#_edn3

Acedido em: 24/11/2011.

Koblentz, E.,(2011) "Government Modernizing Software Forensics Database"

Law Technology News November 17, 2011

Disponível em: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN jsp?id=1202532647567&Government_Modernizing_Software_Forensics_Database&slreturn=1

Acedido em: 24/11/2011.

Koehler, R., (2005) - Elementary Computer Mathematics – Disk Geometry

E-book Publicado pela University of Cincinnati

Kruse, W. , Heiser, G., (2002). Computer forensics incident response essentials

Addison-Wesley Professional; 1 edition

Landis, H.,(2002) "How it Works: Master Boot Record."

Disponível em: http://www.ata-atapi.com/hiwtab.html

Acedido em: 21/1/2012

Metz, J., (2006) - Expert Witness Compression Format specification

Disponível em: http://switch.dl.sourceforge.net/project/libewf/documentation/EWF file format/Expert Witness Compression Format (EWF).pdf

Acedido em: 3/2/2012.

Microsoft, (2007). Identifiers Generated by USBSTOR.SYS.

Disponível em: http://msdn2.microsoft.com/en-us/library/ms791086.aspx

Acedido em: 19/9/2011.

National Software Reference Library [NSRL], (2011)

Disponível em: http://www.nsrl.nist.gov/index.html

Acedido em: 19/6/2011.

NFC - The National Fraud Center, Inc. (2010) "The Growing Global Threat of Economic and Cyber Crime" In conjunction with The Economic Crime Investigation Institute Utica College

Palmer, Gary L..(2001) "A Road Map for Digital Forensic Research".

Technical Report DTR-T001-01, DFRWS, November 2001

Report From the First Digital Forensic Research Workshop (DFRWS).

Pimenta, C. (2009) "Esboço de Quantificação da Fraude em Portugal"

Working Papers Nº 3/2009 OBEGEF – Observatório de Economia e Gestão de Fraude

Prasad, G., (2001.) "*Open Source*-onomics: Examining some pseudo-economic arguments about

Open Source."

Disponível em: http://www.linuxtoday.com/infrastructure/mailprint.php3?action=pv&ltsn=2001-04-12-006-20-OP-BZ-CY

Acedido em: 9/8/2011.

Pwc, (2011) - Global economic crime survey 2011

Disponível em: http://www.pwc.com/gx/en/economic-crime-survey/download-economic-crime-people-culture-controls.jhtml

Acedido em: 9/8/2011.

Richard, G. e Roussev V. (2005) Scalpel: A frugal, high performance file carver

In Proceedings of the 2005 Digital Forensics Research Workshop - DFRWS, August 2005

Disponível em: http://www.digitalforensicssolutions.com/Scalpel/

Acedido em: 04/6/2011.

Ruibin G., Yun K. e Gaertner M., (2005) - Binding Computer Intelligence to the Current Computer Forensic Framework

Disponível em:

http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A6A102-A93D-85B1-96C575D5E35F3764.pdf

Acedido em: 04/11/2011

Rynearson J., (2002) - Evidence and Crime Scene Reconstruction.

National Crime Investigation and Training, sixth edition,.

Schneier, B , (2004) "Secrets and Lies - Digital Security in a Networked World"

Wiley Computer Publishing, Inc

Sheldon B., (2003) - Forensic analysis of Windows systems.

Handbook of computer crime investigation. Academic Press;

Sommer, P., (2010) – "Forensic Science Standards in Fast-Changing Environments"

London School of Economics & Political Science, Open University, UK

Disponível em: http://www.pmsommer.com/page7.html

Acedido em: 24/9/2011

Stallman,R., (2011) "Copyleft: Pragmatic Idealism Free Software Foundation. Philosophy of the GNU Project"

Disponível em: http://www.gnu.org/philosophy/philosophy.html

Acedido em: 19/6/2011.

StatCouter-Global Stats (2012) – Top 5 Operating Systems

Disponível em: http://gs.statcounter.com/#os-ww-monthly-201102-201202

Acedido em: 12/3/2012

SWGDE1, (2011) - Best Practices for Computer Forensics

Disponivel em: http://www.swgde.org/documents/current-documents/

Acedido em: 08/12/2011

SWGDE2, (2009) - Digital Multimedia Evidence Glossary v2.3

Disponível em: http://www.swgde.org/documents/archived-documents/2009-05-22%20SWGDESWGIT%20Digital%20%20Multimedia%20Evidence%20Glossary%20v2.3.pdf

Acedido em: 08/12/2011

UNODC, (2005) - Economic and Financial Crimes: Challenges to Sustainable Development

Disponível em: http://www.unis.unvienna.org/pdf/05-82108_E_5_pr_SFS.pdf

Acedido em: 22/05/2011.

UNODC, (2009) - Fraude financeira e falsificação de identidade: combatendo uma perigosa nova "aliança"

Disponível em: http://www.unodc.org/brazil/pt/pressrelease_20090430.html

Acedido em: 22/05/2011.

Vacca, J., (2005) – Computer Forensics – Computer Crime scene Investigation 2.ª Edição

Publicado pela editora Charles River Media - ISBN: 1-58450-389-0

Wheeler, D., (2003)"Secure Programming for Linux and Unix HOWTO" V3.010

Disponível em: http://www.dwheeler.com/secure-programs/

Acedido em;- 28/6/2011.

Wang, S., (2007) - Measures of retaining digital evidence to prosecute computer-based cyber-crimes - Computer Standards & Interfaces 29(2): 216-223 (2007)

Wang, X., Feng, D., Lai,X. e Yu, H., (2004)

"Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD"

Disponível em: http://eprint.iacr.org/2004/199.pdf

Acedido em:04/6/2011.

Zuboff, S., (2009) - Wall Street's Economic Crimes Against Humanity

BusinessWeek – VIEWPOINT - March 20, 2009

Disponível em:http://www.businessweek.com/managing/content/mar2009/ca20090319_591214.htm

Acedido em;- 22/5/2011.

ANEXO I

PLATAFORMA DE ANÁLISE:

A1. DEFINIÇÃO DA PLATAFORMA DE ANÁLISE

Pretende-se que a plataforma de análise inclua em exclusivo ferramentas "*open source*". Parte destas ferramentas são distribuídas em código fonte ou sob a forma de scripts desenvolvidos em linguagens interpretadas, o que implica, para o primeiro caso a necessidade de gerar o correspondente código executável e para o segundo, a necessidade de dispor dos interpretadores adequados. Este capítulo trata dos aspectos a ter em conta em termos da configuração base necessária para a realização de exames com ferramentas de código aberto usando Linux.

A1.1. AMBIENTE DE DESENVOLVIMENTO

No que respeita ao ambiente de desenvolvimento, este pode ser o ambiente genérico usado para construir aplicações de código aberto escritas em C e C + +, assegurando a instalação das bibliotecas necessárias ao funcionamento das aplicações.

```
mdelgado@CM17MOSS2012:~$ sudo apt-get install build-essential
[sudo] password for mdelgado:
A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto
...
```

Assegurada a instalação do nosso ambiente de desenvolvimento, segue-se a instalação das bibliotecas específicas necessárias para muitas das ferramentas de que iremos mais tarde necessitar. Por norma as aplicações de código aberto são acompanhadas de um documento de referência, (README ou INSTALL), que contem informações a respeito das eventuais bibliotecas de que dependem, sendo indispensável a sua consulta antes de desencadear o processo de compilação.

O processo de construção de um módulo envolve três etapas sequenciais:

1. ./configure;
2. make;
3. (sudo) make install.

A primeira delas, consubstancia-se num script que acompanha o código que tem por objectivo elencar as eventuais opções de configuração.

A1.2. LIBEWF

Uma das bibliotecas de referência na área da Informática Forense é a "Libewf", que pode ser descarregada de: *http://sourceforge.net/projects/libewf/files/libewf/libewf-20100226/*.

A título de exemplo, serão descritos os passos necessários para a instalação deste módulo. Acedendo à opção help do script de configuração que acompanha esta biblioteca temos:

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ ./configure --help

`configure' configures libewf 20100226 to adapt to many kinds of systems.

Usage: ./configure [OPTION]... [VAR=VALUE]...
To assign environment variables (e.g., CC, CFLAGS...), specify them as
VAR=VALUE.  See below for descriptions of some of the useful variables.
--enable-wide-character-type
                        enable wide character type support (default is no)
 --enable-static-executables
                        build the ewftools as static executables (default is no)
 --enable-low-level-functions
                        use libewf's low level read and write functions in the ewftools (default is no)
```

O output, truncado dada a extensão, prossegue com um vasto conjunto de opções.

A instalação da livraria, inicia-se com o script "**configure**":

```
 mdelgado@CM17MOSS2012:~/src/libewf-20100226$ ./configure --enable-wide-character-type --enable-low-level-functions
 checking for a BSD-compatible install... /usr/bin/install -c
 checking whether build environment is sane... yes
 …
```

Concluído o processo de configuração, lança-se o comando "**make**":

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ make

Making all in include
make[1]: Entering directory `/home/mdelgado/src/libewf-20100226/include'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/home/mdelgado/src/libewf-20100226/include'
…
```

Segue-se o comando "**make install**":

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ sudo make install
[sudo] password for mdelgado:

Making install in include
make[1]: Entering directory `/home/mdelgado/src/libewf-20100226/include'
make[2]: Entering directory `/home/mdelgado/src/libewf-20100226/include'
…
```

A1.3. INTERPRETADORES

No que respeita aos scripts, normalmente escritos em Perl, Python ou Ruby, para a respectiva execução vamos necessitar dos interpretadores apropriados bem como, de meios para instalar módulos que constituam pré-requisitos de que as aplicações dependem.

Para verificar a versão instalada do "perl":

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ perl -v

This is perl 5, version 12, subversion 4 (v5.12.4) built for i686-linux-gnu-thread-multi-64int
(with 45 registered patches, see perl -V for more detail)
…
```

Para verificar a versão instalada do "python":

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ python -V
Python 2.7.2+
```

Relativamente ao python dada a grande evolução das versões 2.X para a 3, que não garante rectro-compatibilidade para scripts escritos em versões anteriores, é conveniente dispor das duas versões, pelo que se deve assegurar igualmente a instalação da versão 3.

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ sudo apt-get install python3-minimal
[sudo] password for mdelgado:

A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto
…
```

Para verificar a versão instalada do “ruby”:

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ ruby -v
A aplicação 'ruby' poderá ser encontrada nos seguintes pacotes:
 * ruby1.8
 * ruby1.9.1
Tente: sudo apt-get install <pacote selecionado>
```

A resposta indica-nos que o “ruby” não está instalado.

Para assegurar a respectiva instalação teremos:

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ sudo apt-get install rubygems

A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto

Os seguintes pacotes foram instalados automaticamente e já não são necessários:
  gir1.2-timezonemap-1.0 archdetect-deb python-pyicu python-argparse
  libdebian-installer4 rdate python-xklavier btrfs-tools localechooser-data
  apt-clone libtimezonemap1 dpkg-repack libdebconfclient0
…
```

A1.4. FUSE[7]

O FUSE é um módulo do kernel Linux que permite a interpretação do "sistemas de ficheiros em modo utilizador." Adicionalmente, alguns módulos FUSE também permitem interpretar volumes ou contentores possibilitando o acesso ao respectivo conteúdo. Existem módulos FUSE para diversas implementações, desde sistemas baseados na cloud, sistemas de ficheiros locais encriptados, Wikipedia como um sistema de ficheiros, etc. Podemos instalar alguns módulos FUSE recorrendo ao seguinte comando:

```
mdelgado@CM17MOSS2012:~/src/libewf-20100226$ sudo apt-get python-fuse fuse-zip sshfs
[sudo] password for mdelgado:
```

[7] http://fuse.sourceforge.net/

```
A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto
Os seguintes pacotes foram instalados automaticamente e já não são necessários:
gir1.2-timezonemap-1.0 archdetect-deb python-pyicu python-argparse libdebian-installer4
rdate python-xklavier btrfs-tools localechooser-data apt-clone libtimezonemap1
dpkg-repack libdebconfclient0
…
…
```

Deste modo instalamos:

- Python FUSE – Uma API Python que permite a implementação de sistemas de ficheiros FUSE;
- Fuse-Zip – Um módulo FUSE que permite apresentar um ficheiro ZIP como um sistema de ficheiros;
- SSHFS - Um módulo FUSE que de forma transparente permite apresentar um sistema de ficheiros remoto como sistema de ficheiros local sobre SSH(SFTP/SCP);

A1.5. MOUNT_EWF

MountEWF permite apresentar uma imagem no formato contentor EWF, (Expert Witness Format), como uma imagem RAW. Esta funcionalidade tem por base o sistema FUSE via Python. Trata-se de um módulo que faz parte do projecto LibEWF.

Um contentor do tipo EWF, pode conter múltiplos sistemas de ficheiros montáveis, o que impossibilita a respectiva "montagem" de forma directa. O MountEWF proporciona a separação dos diversos componentes integrados no contentor, permitindo que estes possam ser montados individualmente.

Trata-se de um script python que não carece de compilação, bastando, após fazer o respectivo download, assegurar a respectiva transferência para um local /usr/local/Bin, de modo a facilitar a execução.

```
mdelgado@CM17MOSS2012:~$ cd /usr/local/bin
mdelgado@CM17MOSS2012:/usr/local/bin$ sudo cp ~/Transferências/mount_ewf-20090113.py .
```

```
[sudo] password for mdelgado:
mdelgado@CM17MOSS2012:/usr/local/bin$ ls -al
total 1884
drwxr-xr-x  6 root root   4096 2012-03-18 08:36 .
drwxr-xr-x 10 root root   4096 2011-12-07 12:54 ..
…
-rw-r--r--  1 root root  15556 2012-03-18 08:36 mount_ewf-20090113.py
…
```

Vamos renomear o script e atribuir permissão de execução, para facilitar o uso:

```
mdelgado@CM17MOSS2012:/usr/local/bin$ sudo mv mount_ewf-20090113.py mountewf.py

mdelgado@CM17MOSS2012:/usr/local/bin$ sudo chmod 755 mountewf.py

mdelgado@CM17MOSS2012:/usr/local/bin$ ls -al
total 1884
drwxr-xr-x  6 root root   4096 2012-03-18 08:36 .
drwxr-xr-x 10 root root   4096 2011-12-07 12:54 ..
…
-rwxr-xr-x  1 root root  15556 2012-03-18 08:36 mountewf.py
…
```

Vamos testar com a imagem usada no CENÁRIO- 4:

```
mdelgado@CM17MOSS2012:/usr/local/bin$ cd ~
mdelgado@CM17MOSS2012:~$ mkdir MountPoint
mdelgado@CM17MOSS2012:~$ mountewf.py /media/KINGSTON/MOSS/CASE-4-MOSS-
2GB.E01 ./MountPoint/

Using libewf-20100226. Tested with libewf-20080501.

mdelgado@CM17MOSS2012:~$ ls -lath MountPoint/

total 2,0G
drwxr-xr-x 28 mdelgado mdelgado 4,0K 2012-03-18 08:41 ..
dr-xr-xr-x  2 root     root        0 1970-01-01 01:00 .
-r--r--r--  1 root     root     2,0G 1970-01-01 01:00 CASE-4-MOSS-2GB
-r--r--r--  1 root     root      387 1970-01-01 01:00 CASE-4-MOSS-2GB.txt
```

A imagem, sendo um contentor EWF, engloba um bloco de meta-dados que o Mout_Ewf reconhece e separa no ficheiro CASE-4-MOSS-2GB.txt, cujo conteúdo podemos ver:

```
mdelgado@CM17MOSS2012:~$ cat ./MountPoint/CASE-4-MOSS-2GB.txt
# Description: FDiskedDrive2GB
# Case number: AdvCncptsCH10
# Examiner name: Bunting
# Evidence number: FDiskedDrive2GB
# Notes: NTFS and FAT32 partitions removed with fdisk
# Acquiry date: 2005-09-19T17:20:16
# System date: 2005-09-19T17:20:16
# Operating system used: Windows XP
# Software version used: 5.04
fe1e312cce4961e35a595f61ebae0aa3 */home/mdelgado/MountPoint/CASE-4-MOSS-2GB

mdelgado@CM17MOSS2012:~$
```

A1.6. AFFUSE

De forma idêntica ao Mount_EWF, o módulo AFFuse, permite apresentar uma imagem no formato contentor AFF, (Advanced Forensic Format), como uma imagem RAW. Trata-se de um módulo que faz parte do projecto que faz parte da AFF library, disponível em www.afflib.org.

A sua instalação passa pela instalação dos dois módulos seguintes:

```
mdelgado@CM17MOSS2012:~$ sudo apt-get install libfuse-dev libexpat1-dev
[sudo] password for mdelgado:

A ler as listas de pacotes... Pronto
A construir árvore de dependências
A ler a informação de estado... Pronto
Os seguintes pacotes foram instalados automaticamente e já não são necessários:
…
Os seguintes pacotes extra serão instalados:
  libselinux1-dev libsepol1-dev
Serão instalados os seguintes NOVOS pacotes:
```

```
  libexpat1-dev libfuse-dev libselinux1-dev libsepol1-dev
0 pacotes actualizados, 4 pacotes novos instalados, 0 a remover e 230 não actualizados.
É necessário obter 1188 kB de arquivos.
…
Após esta operação, serão utilizados 4452 kB adicionais de espaço em disco.
Deseja continuar [Y/n]? y
…
mdelgado@CM17MOSS2012:~$
```

A1.7. XMOUNT

XMount é similar aos módulos anteriores, (MountEWF e AFFuse), na medida em que, proporciona ao examinador acesso "RAW" a ficheiros do tipo contentor. A grande diferença está na particularidade de, em lugar de apresentar simplesmente o resultado no formato "dd", o XMount possibilita a apresentação do conteúdo do contentor nos formatos VirtualBox ou VMWare através da conversão em tempo real via FUSE, o que se revela de extrema utilidade num ambiente de análise baseado em Linux, pois permite iniciar uma instância virtual a partir da imagem de um sistema.

A instalação é assegurada da seguinte forma:

```
mdelgado@CM17MOSS2012:~$ sudo aptitude install xmount
[sudo] password for mdelgado:

Os seguintes NOVOS pacotes serão instalados:
  xmount

Os seguintes pacotes serão REMOVIDOS:
…
0 pacotes actualizados, 1 novos instalados, 13 para serem removidos e 230 não actualizados.
É preciso obter 30,1 kB de ficheiros. Depois de desempacotar, serão libertados 4809 kB.
Deseja continuar ? [Y/n/?] y

Obter: 1 http://ftp.caixamagica.pt/caixamagica/ finisterra/universe xmount i386 0.4.5-1 [30,1 kB]
Fetched 30,1 kB in 0s (107 kB/s)
(A ler a base de dados ... 178345 ficheiros e directórios actualmente instalados.)
A remover apt-clone ...
…
A processar 'triggers' para man-db ...
```

```
…
A seleccionar pacote anteriormente não seleccionado xmount
(A ler a base de dados ... 178174 ficheiros e directórios actualmente instalados.)
A descompactar xmount (desde .../xmount_0.4.5-1_i386.deb) ...
A processar 'triggers' para man-db ...
A instalar xmount (0.4.5-1) ...
```

Testar o processo de montagem simples:

```
mdelgado@CM17MOSS2012:~$ sudo xmount --in ewf /media/KINGSTON/MOSS/CASE-4_MOSS-2GB.E01 /mnt
mdelgado@CM17MOSS2012:~$ ls -al /mnt
total 4
drwxrwxrwx  2 root root          0 1970-01-01 01:00 .
drwxr-xr-x 23 root root       4096 2012-03-17 11:18 ..
-r--r--r--  1 root root 2111864832 1970-01-01 01:00 CASE-4_MOSS-2GB.dd
-r--r--r--  1 root root        388 1970-01-01 01:00 CASE-4_MOSS-2GB.info
```

Tal como se verificou com o MountEwf, o ficheiro *.info contém os meta-dados associados ao contentor.

Testar o processo de montagem com imagem virtual do tipo Virtualbox:

```
mdelgado@CM17MOSS2012:~$ sudo xmount --in ewf --out vdi
                                /media/KINGSTON/MOSS/CASE-4_MOSS-2GB.E01 /mnt
mdelgado@CM17MOSS2012:~$ ls -al /mnt

total 4
drwxrwxrwx  2 root root          0 1970-01-01 01:00 .
drwxr-xr-x 23 root root       4096 2012-03-17 11:18 ..
-r--r--r--  1 root root        388 1970-01-01 01:00 CASE-4_MOSS-2GB.info
-r--r--r--  1 root root 2111873404 1970-01-01 01:00 CASE-4_MOSS-2GB.vdi

mdelgado@CM17MOSS2012:~$
```

Um dos principais pontos fortes do uso do Linux como uma plataforma de análise forense consiste na grande variedade de sistemas de ficheiros suportados como módulos

do kernel. O Ubuntu, actual base da distribuição Caixa Mágica 17, tem dezenas de sistemas de arquivos disponíveis, como módulos passíveis de carregar no kernel, como se pode verificar, consultando a secção "File Systems" do ficheiro "/boot/config-3.0.0-13-generic".

A1.8. FERRAMENTAS PARA REALIZAÇÃO DE IMAGENS

O comando "**dd**" é a ferramenta de código aberto mais básica para criar uma imagem forense de que dispomos. Dado que este comando está universalmente presente nos sistemas operativos da família Unix, constitui a base para vários outros utilitários concebidos para este fim, pelo que, conhecer o seu princípio de funcionamento é extremamente importante para quem pretende aventurar-se no mundo da Informática Forense.

O objectivo básico do comando "**dd**" é assegurar a cópia de dados de um lugar para outro. Contudo, o utilizador pode fornecer diversos argumentos e flags para modificar essa função base, mostrando-se bastante clara a sintaxe básica da ferramenta.

Para fazer um clone simples de uma unidade para outra, basta invocar a ferramenta deste modo:

```
mdelgado@CM17MOSS2012:~$ sudo dd if = /dev/sda  of =/dev/sdb  bs = 4096
```

São lidos 4096 bytes de cada vez a partir do primeiro local, e gravados de seguida no segundo local. Se não for fornecido o tamanho do bloco (bs =), o comando assume que este corresponde a um sector, ou seja, (bs=512).

dcfldd - Desenvolvido pelo (Defense Computer Forensic Laboratory) o dcfldd é uma versão do dd projectada especificamente para uso forense. Trata-se de um fork do GNU dd, com um modo de funcionamento muito semelhante, embora acrescente um conjunto de recursos, nomeadamente para cálculo do hash, validação, registo da actividade e segmentação do arquivo de output em partes de tamanho fixo, o que se revela bastante conveniente face à dimensão dos actuais discos.

O comando seguinte, refaz a imagem feita anteriormente com o "dd", mas agora criando um log dos hashes MD5 e SHA1 gerados a partir de cada bloco de 512 MB.

```
mdelgado@CM17MOSS2012:~$ sudo dcfldd bs=32k if=/dev/sdg of=dcfldd.img
hashwindow=512M hash=md5,sha1 hashlog=dcfldd.hashlog
60672 blocks (1896Mb) written.
60832+0 records in
60832+0 records out
```

dc3dd - Desenvolvido pelo (Department of Defense Cyber Crime Center), é um patch sobre o GNU dd, também projectado especificamente para uso forense. Funciona de forma muito semelhante ao dcfldd, embora comporte funcionalidades adicionais.

Ewfaquire - ewfacquire é um utilitário desenvolvido especificamente para possibilitar a aquisição de dados a partir de uma fonte e armazená-los em contentores no formato EWF (Expert Witness Compression Format). (EnCase, n.d.).

O formato EWF é amplamente utilizado no domínio da informática forense para armazenar imagens, nomeadamente por duas das mais utilizadas ferramentas comerciais de análise forense: EnCase, da Guidance Software (http://www.guidancesoftware.com/) e o Forensic Tool Kit (FTK) da Access Data (http://www.accessdata.com/) (Carlton, 2008).

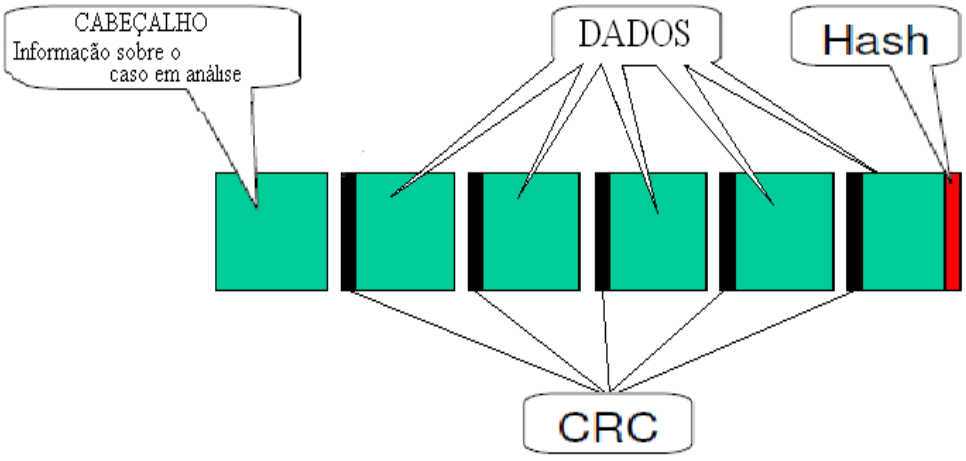

Figura A1-1 – Expert Witness Compression Format com base em (Metz, 2006)

Embora se trate de uma ferramenta de linha de comando, a sua utilização é extremamente intuitiva, conforme se pôde constatar no exemplo descrito em 6. 1. 3, no qual recorremos a esta ferramenta para realização da imagem pericial respeitante ao CENÁRIO- 1.

Guymager - É um utilitário com interface gráfica, desenvolvido para criação de imagens forenses, que permite gerar imagens em três formatos distintos: "raw" (tipo dd), AFF (Advanced Forensic Format) e EWF (Expert Witness Compression Format). Para criar imagens neste último formato recorre à LibEWF.

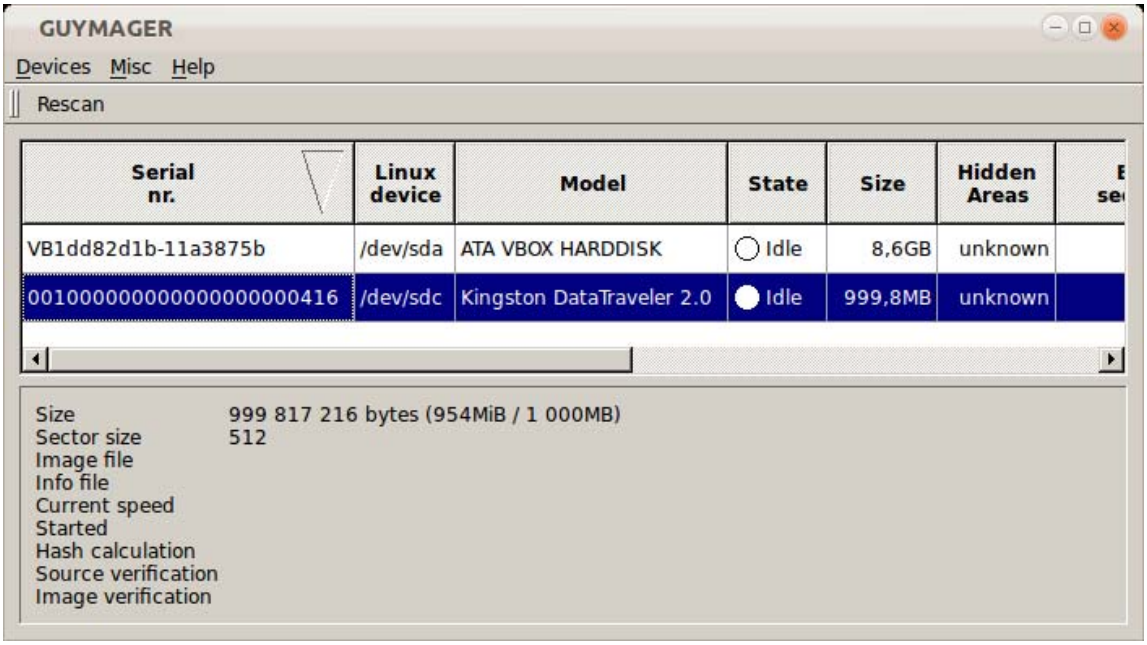

Figura A1-2 – Interface principal do Guymager

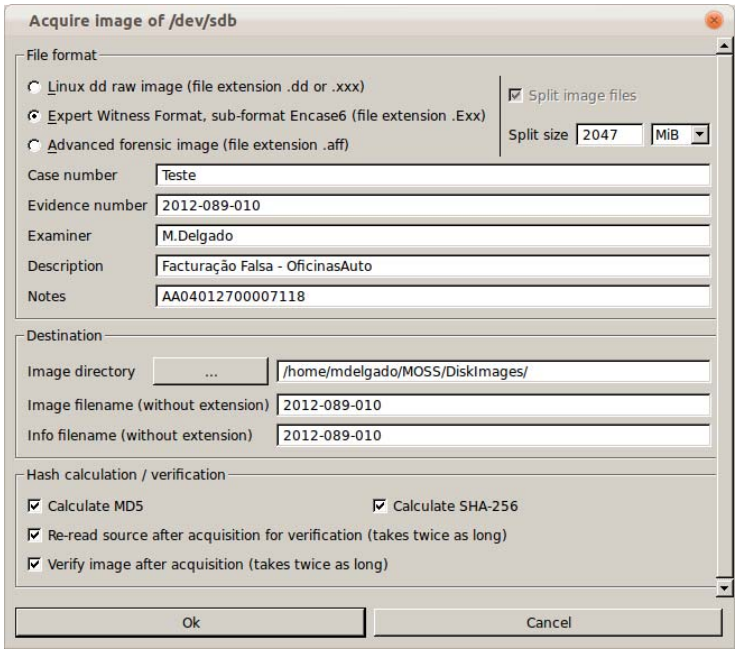

Figura A1-3 – Interfaces Acquire do Guymager

A1.9. FERRAMENTAS PARA ANÁLISE

Conforme referido em 4.4, os dispositivos de armazenamento em massa (Discos rígidos e afins), constituem dispositivos chave na investigação de crimes económicos. A análise destes dispositivos tem por objectivo identificar, extrair e analisar os ficheiros e sistemas de ficheiros em que os mesmos residem.

Identificar, implica determinar ficheiros activos e apagados, existentes no dispositivo.

Extrair, implica recuperar dados e meta-dados relevantes para o caso sob investigação.

Por fim, no processo de análise, através da inteligência e raciocínio lógico do examinador, são estabelecidas ligações entre as provas recolhidas de modo a reconstruir os eventos criminalizáveis.

São assim necessárias ferramentas para a realização de imagens destes dispositivos e ferramentas com capacidades para analisar os diferentes tipos de sistemas de ficheiros existentes, mormente os mais comuns.

A1.9.1 TEST DISK / PHOTOREC

O TestDisk é um poderoso software *open source* para recuperação de dados, desenhado especialmente para facilitar a recuperação de partições perdidas e recuperação de discos de arranque. O Photorec, é vocacionado para a recuperação de ficheiros perdidos, incluindo vídeo, documentos etc. Este software ignora o sistema de ficheiros do dispositivo alvo, possibilitando a recuperação de informação gravada em qualquer dispositivo de armazenamento que possa ser lido através do computador, como CD/DVD-ROM, Memórias flash de câmaras digitais etc.

Ambos de utilização simples e intuitiva conforme se constata da sua utilização nos exemplos práticos constantes do capítulo 6.

A1.9.2 THE SLEUTH KIT

O Sleuth Kit (TSK) é uma suite de ferramentas *open source*, disponível em http://www.sleuthkit.org/sleuthkit/download.php, para análise forense de file systems, desenvolvida originalmente por Brian Carrier, que integra diversos módulos de linha de comando, os quais possibilitam a análise forense de diferentes plataformas Windows e UNIX, nomeadamente: FreeBSD, Linux, Mac OS X, OpenBSD e Solaris, suportando

diversos tipos de sistemas de ficheiros (FAT32, NTFS, UFS, Ext2 e Ext3) Carrier (2003-A).

Este conjunto de ferramentas que actuam a baixo nível, foram projectadas para realizar tarefas autónomas. Contudo, quando usadas em conjunto, permitem realizar um exame completo não-intrusivo, pois não contam com o sistema operativo do dispositivo suspeito para acesso ao respectivo sistema de ficheiros, tornando assim possível aceder a conteúdos apagados e escondidos.

A1.9.2.1 PRINCIPAIS FUNCIONALIDADES

De entre o conjunto de funcionalidades disponibilizadas pelo Sleuth Kit destacam-se:

- Listagem de nomes de ficheiros alocados (acessíveis via file system), e ficheiros apagados (fora do controlo do file system);
- Mostra os detalhes e conteúdo de todos os atributos do sistema de ficheiros NTFS (Incluindo Alternate Data Streams);
- Mostra o Sistema de Ficheiros e detalhas da respectiva estrutura de meta-dados;
- Criação de cronogramas de atividade de ficheiros, que podem ser importados para uma folha de cálculo permitindo criar gráficos e relatórios;
- Permite organizar arquivos com base no respectivo tipo (separação de ficheiros executáveis, imagens e documentos de texto)
- Permite, ainda, criar páginas de thumbnails para facilitar e agilizar a análise de imagens.

A1.9.2.2 CAMADAS DO "THE SLEUTH KIT"

Trabalhar com um conjunto extenso de ferramentas de linha de comando autónomas, nem sempre é uma tarefa fácil. No caso do Sleuth Kit, Carrier, fiel à sua abordagem por camadas, procurou facilitar a tarefa agrupando as ferramentas de forma lógica, em função da camada do file system que cada uma delas visa. Temos assim as seguintes camadas: Volume Layer, File System Layer, Data Unit Layer, Metadata Layer e File Name Layer, Carrier (2003-B).

A1.9.2.3 VOLUME

Conforme referido no capítulo 4, um volume comporta parte ou a totalidade do espaço de uma ou mais unidades de disco, sendo que uma unidade de disco pode conter vários

volumes. A Volume Layer do TSK, é responsável pela manipulação de volumes, destacando-se nesta camada a ferramenta:

- **mmls** que efectua a análise e mostra a estrutura de gestão da imagem ou do próprio dispositivo. Contrariamente ao fdisk, o mmls mostra claramente o espaço não alocado antes, depois e entre volumes.

```
mdelgado@mdelgado-VirtualBox:~/MOSS/DiskImg$ mmls 10-ntfs-disk.dd ([8])

DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0000096389   0000096327   NTFS (0x07)
03:  00:01   0000096390   0000192779   0000096390   NTFS (0x07)
04:  -----   0000192780   0000192783   0000000004   Unallocated
```

Podemos, através deste exemplo, verificar os elementos que o comando "mmls" nos fornece:

1. A Partition Table está no primeiro sector do disco "00";
2. Os 63 primeiros sectores não estão alocados;
3. Estão presentes duas partições. A primeira entre os sectores 63 e 96389 e a segunda entre 96390 e 192779;
4. Os 4 últimos sectores, compreendidos entre 192780 e 192783 não estão alocados.

Os elementos fornecidos por este comando, são extremamente importantes, pois constituem inputs indispensáveis para a extracção de informação das partições, com recurso ao comando "dd".

A1.9.2.4 FILE SYSTEM

Os discos rígidos (ou qualquer outro dispositivo de armazenamento) são divididos em partições (uma ou mais), comportando cada uma delas, uma estrutura lógica de armazenamento e organização de dados (file system).

[8] Retirado de http://dftt.sourceforge.net/test10/index.html

A File System Layer do TSK, é responsável por manipular essas estruturas de dados. O conjunto de ferramentas associadas a esta camada, são identificadas facilmente pelo prefixo "fs".

Um dos mais importantes é o fsstat, responsável por mostrar informações como: nome do volume, estrutura, tamanho, data da última montagem, entre outros elementos.

```
mdelgado@mdelgado-VirtualBox:~/MOSS/DiskImages$ fsstat ubnist1.casper-
rw.gen3.aff
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: 9935811771d9768b49417b0b3b881787

Last Written at: Tue Jan  6 18:59:33 2009
Last Checked at: Sun Dec 28 20:37:56 2008

Last Mounted at: Tue Jan  6 18:59:33 2009
Unmounted properly
Last mounted on:

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery,
Read Only Compat Features: Sparse Super, Has Large Files,
```

Este exemplo mostra parte do output do comando fsstat, destacando-se elementos de grande utilidade para a investigação, como sejam os relacionados com as últimas datas de escrita e de montagem.

A1.9.2.5 DATA UNIT

A Data Unit Layer é aquela em que os ficheiros e directórios são armazenados. Quando o sistema operativo necessita de espaço em disco, aloca unidades de armazenamento (tipicamente, blocos ou clusters). A dimensão destas estruturas varia segundo uma potência de 2: (512, 1024, 4096, etc) bytes. As ferramentas do TSK específicas para esta camada são identificadas pelo prefixo "d", destacando-se:

- O dcat, que exibe o conteúdo de uma unidade de dados (semelhante ao comando cat, do UNIX), o que permite visualizar dados ocultos em áreas não utilizadas normalmente pelo sistema de ficheiros;
- o dls mostra o conteúdo das áreas de disco não alocadas;
- o dstat mostra informações de uma unidade de dados de forma amigável;
- o dcalc é utilizado quando um dado é recuperado pelo dls numa área não alocada e se deseja calcular a sua "posição" no sistema de ficheiros.

A1.9.2.6 META-DATA

As informações dos ficheiros e directórios, descrita pelos inodes nos sistemas UNIX ou pelo MFT (Master File Table) em sistemas NTFS, são da responsabilidade da Metadata Layer. Entre essas informações, estão os tempos de acesso, o tamanho e os endereços de armazenamento dos dados no disco. As ferramentas referentes a esta camada identificam-se com o prefixo "i", destacando-se:

- O ils lista as informações de um dado inode (ou de outro meta-dado, no caso de sistemas diferentes do UNIX). Por norma, listará apenas os ficheiros removidos;
- O icat mostra o conteúdo de um arquivo a partir do seu inode e, combinado com o ils, pode ser utilizado na recuperação de ficheiros apagados;
- O istat exibe informações sobre um determinado inode, tais como tamanho, "MAC times" e identificadores do proprietário;
- O ifind retorna o inode associado a um dado ficheiro ou diretório.

A1.9.2.7 FILE NAME

A camada “File Name” (também conhecida por camada de interface humana), permite uma interacção com os ficheiros de forma mais cómoda do que a camada de meta-dados. As ferramentas relacionadas a esta camada são identificadas pelo prefixo "f", destacando-se:

- O fls lista os arquivos e directórios em uma imagem de disco, mesmo aqueles apagados;
- O ffind faz o oposto do ifind, isto é, a partir de um inode ele identifica o nome do arquivo que é referenciado.

A1.9.2.8 FERRAMENTAS AO NÍVEL DO DISCO

Conforme referido em 4.4.3.1, pode ser usada uma HPA para ocultar dados, pois trata-se de uma área que não seria copiada num processo normal de aquisição. Estas ferramentas podem ser usadas para detectar e remover uma Host Protected Área (HPA) num disco ATA, possibilitando assim a cópia de toda a informação ali gravada. Estão disponíveis dois comandos:

- • 'disk_sreset' - Usa comandos ATA para consultar o disco rígido. Caso exista uma Host Protected área (HPA), remove-a temporariamente para que possa ser feita a aquisição completa do disco. Entretanto, após a reinicialização do disco, a HPA voltará a existir novamente.
- • 'disk_stat' - Usa comandos ATA para consultar o disco rígido. Disponibiliza informação sobre o número real de sectores e se existe no disco uma Host Protected Área (HPA).

A1.9.2.9 FERRAMENTAS AO NÍVEL DA IMAGEM

Trata-se de ferramentas que permitem identificar o formato do arquivo de imagem. Por exemplo, se se trata de uma imagem compactada ou seccionada e diversas partes.

- • 'img_stat' - Exibe os detalhes associados a um ficheiro de imagem. O output desta ferramenta especifíca o formato da imagem. No mínimo, determina o tamanho e identifica o intervalo de bytes de cada arquivo, no caso de formatos de imagens seccionadas.

A1.9.3 AUTOPSY FORENSIC BROWSER

O Autopsy Forensic Browser (Autopsy) é uma interface Web, disponível em http://www.sleuthkit.org/autopsy/download.php, que possibilita a realização da maioria das tarefas do The Sleuth Kit, a partir de uma interface gráfica na qual todas as funções estão acessíveis pelo navegador.

Acrescenta ainda outra funcionalidade extremamente importante que consiste no registo em arquivos de log, de todas as acções realizadas, permitindo auditar posteriormente o processo de investigação desenvolvido.

Figura A1-4 *– Ecran de entrada do Autopsy*

Para cada sistema investigado, o Autopsy requer a criação de um "caso", conforme ilustra a figura, contendo o nome dos investigadores, do dispositivo a analisar e das correspondentes imagens adquiridas. Para cada caso, o Autopsy cria uma estrutura de arquivos e directórios, contendo documentação diversa, (relatórios, logs e outros elementos considerados relevantes).

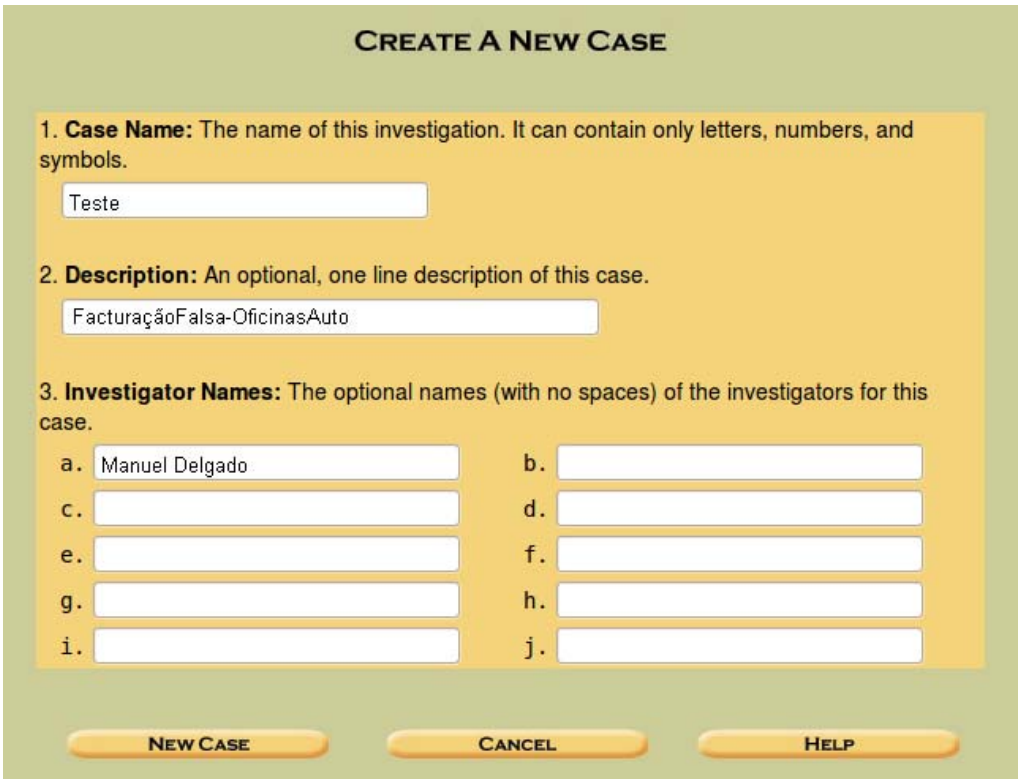

Figura A1-5 *– Criação de um novo "caso" no "Autopsy Forensic Browser".*

Figura A1-6 *– Estrutura de directórios criada para cada caso pelo Autopsy .*

A1.9.4 REGRIPPER

Longe de mais um Registry Viewer, o RegRipper foi desenvolvido para extrair informação residente nos ficheiros de registry previamente copiados dos sistemas suspeitos.

Trata-se de uma ferramenta desenvolvida em Perl por Harlan Carvey, que se destaca pela rapidez e facilidade de utilização, recolhendo a preferência da maioria dos profissionais da Computação Forense, quando pretendem analisar ficheiros de registry.

Recorrendo ao módulo *Parse::Win32Registry*, James McFarlane localiza e acede aos nós fundamentais do Registry, assim como aos respectivos valores e dados. Ao aceder a um nó chave, recupera o valor "LastWrite" traduzindo-o para um formato inteligível, tratando de igual forma os restantes dados.

Para o efeito disponibiliza diversos plugin's que permitem recuperar os diversos tipos de dados e assegurar a respectiva conversão sempre que necessário.

A versão utilizada (V2.02), disponibiliza os seguintes plugin's:

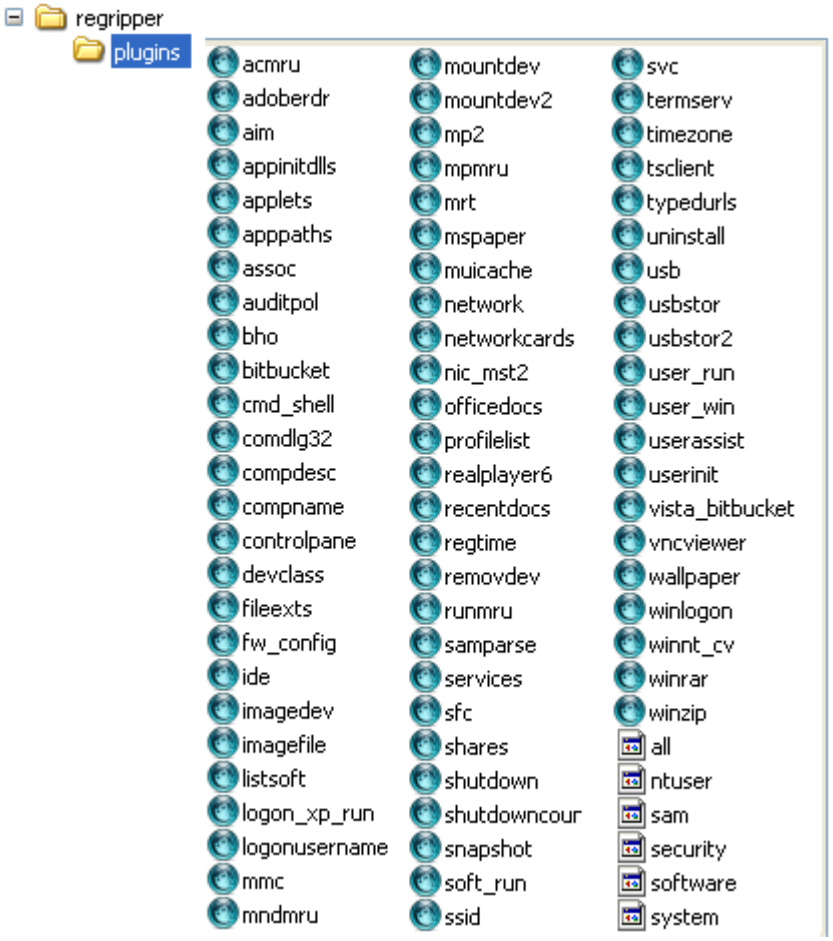

Figura A1-7 *– Plugins do RegRipper .*

A1.9.5 – OUTRAS FERRAMENTAS

Muitas outras ferramentas *Open Source* oferecem, nesta área, performances semelhantes no tratamento de várias outras fontes de evidências digitais, relevantes na investigação do crime económico, tais como:

A1.9.5.1 EVENTLOGPARSER

Script extremamente útil escrito em PHP que permite fazer o parsing dos ficheiros do event log do Windows;

A1.9.5.2 GALLETA

Desenvolvido para examinar o conteúdo dos ficheiros de cookie, fornece os resultados num formato delimitado para facilitar a respectiva análise numa folha de cálculo. Funciona em múltiplas plataformas podendo ser executado no Windows (através do Cygwin), Mac OS X, Linux e plataformas * BSD;

A1.9.5.3 PASCO

Desenvolvido para examinar o conteúdo dos ficheiros de cache do Internet Explorer (index.dat), fornece os resultados num formato delimitado para facilitar a respectiva análise numa folha de cálculo. Funciona em múltiplas plataformas podendo ser executado no Windows (através do Cygwin), Mac OS X, Linux e plataformas * BSD;

A1.9.5.4 LOG2TIMELINE

Framework que permite automatizar o parsing de diversos tipos de ficheiros de log criando uma "*timeline*" para facilitar o processo de análise;

A1.9.5.5 MAC-ROBBER

Utilizado para recolher tempos de Modificação, Acesso e Criação (MAC Times) dos ficheiros de um sistema gerando um output que pode ser utilizado pelo Sleuth Kit para construir uma "*timeline*" que traduza a actividade nesse sistema;

Contudo, o escasso tempo e limitado número de páginas a que a natureza deste trabalho obriga, não permitiu aqui demonstrar.

ANEXO II

CENÁRIO- 2

LogFile do TestDisk:

A2. LOGFILE DO TESTDISK

```
mdelgado@mdelgado-VirtualBox:/media/EnCaseTrain/MOSs$ cat testdisk.log



Sun Feb 26 05:49:56 2012
Command line: TestDisk


TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
OS: Linux, kernel 3.0.0-15-generic (#26-Ubuntu SMP Fri Jan 20 15:59:53 UTC 2012)
Compiler: GCC 4.5 - Oct 17 2010 20:12:36
ext2fs lib: 1.41.14, ntfs lib: 10:0:0, reiserfs lib: none, ewf lib: none
/dev/sda: LBA, LBA48 support
/dev/sda: size       16777216 sectors
/dev/sda: user_max   16777216 sectors
Warning: can't get size for Disk /dev/mapper/control - 0 B - CHS 1 1 1, sector size=512
Hard disk list
Disk /dev/sda - 8589 MB / 8192 MiB - CHS 1044 255 63, sector size=512 - ATA VBOX HARDDISK
Disk /dev/sdb - 120 GB / 111 GiB - CHS 14593 255 63, sector size=512 - TOSHIBA MK1246GSX



TestDisk exited normally.
Using locale 'pt_PT.UTF-8'.



Sun Feb 26 05:51:35 2012
Command line: TestDisk /log Case2-MOSS.001


TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
OS: Linux, kernel 3.0.0-15-generic (#26-Ubuntu SMP Fri Jan 20 15:59:53 UTC 2012)
Compiler: GCC 4.5 - Oct 17 2010 20:12:36
ext2fs lib: 1.41.14, ntfs lib: 10:0:0, reiserfs lib: none, ewf lib: none
Hard disk list
```

```
Disk Case2-MOSS.001 - 2111 MB / 2014 MiB - CHS 257 255 63, sector
size=512


Partition table type (auto): Intel
Disk Case2-MOSS.001 - 2111 MB / 2014 MiB
Partition table type: Intel


Analyse Disk Case2-MOSS.001 - 2111 MB / 2014 MiB - CHS 257 255 63
Current partition structure:
No partition is bootable
Using locale 'pt_PT.UTF-8'.



Sun Feb 26 10:27:50 2012
Command line: TestDisk /log Case2-MOSS.001


TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
OS: Linux, kernel 3.0.0-15-generic (#26-Ubuntu SMP Fri Jan 20 15:59:53
UTC 2012)
Compiler: GCC 4.5 - Oct 17 2010 20:12:36
ext2fs lib: 1.41.14, ntfs lib: 10:0:0, reiserfs lib: none, ewf lib:
none
Hard disk list
Disk Case2-MOSS.001 - 2111 MB / 2014 MiB - CHS 257 255 63, sector
size=512


Partition table type (auto): Intel
Disk Case2-MOSS.001 - 2111 MB / 2014 MiB
Partition table type: Intel


Analyse Disk Case2-MOSS.001 - 2111 MB / 2014 MiB - CHS 257 255 63
Current partition structure:
No partition is bootable
Ask the user for vista mode
Allow partial last cylinder : Yes
search_vista_part: 1


search_part()
Disk Case2-MOSS.001 - 2111 MB / 2014 MiB - CHS 257 255 63
     HPFS - NTFS              0   1  1   127 254 63    2056257
[NTFSBoot]
```

```
     NTFS, 1052 MB / 1004 MiB
     FAT32                 128   0  1   255 254 63    2056320
[HACKTOOLS]
     FAT32, 1052 MB / 1004 MiB
get_geometry_from_list_part_aux head=255 nbr=4
get_geometry_from_list_part_aux head=8 nbr=4
get_geometry_from_list_part_aux head=16 nbr=4
get_geometry_from_list_part_aux head=32 nbr=4
get_geometry_from_list_part_aux head=64 nbr=4
get_geometry_from_list_part_aux head=128 nbr=4
get_geometry_from_list_part_aux head=240 nbr=4
get_geometry_from_list_part_aux head=255 nbr=4

interface_write()
 1 * HPFS - NTFS              0   1  1   127 254 63    2056257
[NTFSBoot]
 2 P FAT32                 128   0  1   255 254 63    2056320
[HACKTOOLS]
write!
No extended partition
You will have to reboot for the change to take effect.

TestDisk exited normally.
```

ANEXO III

CENÁRIO- 5

Output do UVCVIEWER:

A3. RELATÓRIO DO UTILITÁRIO UVCVIEWER.

```
          ---===>Device Information<===---
English product name: "SanDisk Cruzer"

ConnectionStatus:
Current Config Value:              0x01  -> Device Bus Speed: High
Device Address:                    0x01
Open Pipes:                           2

          ===>Endpoint Descriptor<===
bLength:                           0x07
bDescriptorType:                   0x05
bEndpointAddress:                  0x81  -> Direction: IN -
EndpointID: 1
bmAttributes:                      0x02  -> Bulk Transfer Type
wMaxPacketSize:                  0x0200 = 0x200 max bytes
bInterval:                         0x00

          ===>Endpoint Descriptor<===
bLength:                           0x07
bDescriptorType:                   0x05
bEndpointAddress:                  0x02  -> Direction: OUT -
EndpointID: 2
bmAttributes:                      0x02  -> Bulk Transfer Type
wMaxPacketSize:                  0x0200 = 0x200 max bytes
bInterval:                         0x00

          ===>Device Descriptor<===
bLength:                           0x12
bDescriptorType:                   0x01
bcdUSB:                          0x0200
bDeviceClass:                      0x00  -> This is an Interface Class
Defined Device
bDeviceSubClass:                   0x00
bDeviceProtocol:                   0x00
bMaxPacketSize0:                   0x40 = (64) Bytes
idVendor:                        0x0781 = SanDisk Corporation
idProduct:                       0x5530
bcdDevice:                       0x0200
iManufacturer:                     0x01
     English (United States)  "SanDisk"
```

```
iProduct:                           0x02
     English (United States)  "SanDisk Cruzer"
iSerialNumber:                      0x03
     English (United States)  "35501313BA936DC8"
bNumConfigurations:                 0x01

          ===>Configuration Descriptor<===
bLength:                            0x09
bDescriptorType:                    0x02
wTotalLength:                     0x0020  -> Validated
bNumInterfaces:                     0x01
bConfigurationValue:                0x01
iConfiguration:                     0x00
bmAttributes:                       0x80  -> Bus Powered
MaxPower:                           0x64 = 200 mA
```