Definição de informática forense

Em português não existe uma expressão concreta para definir informática forense, sendo que em inglês é utilizado o termo "Computer Forensic".

Entenda-se **Informática Forense** como um ramo da ciência forense relacionado com provas digitais descobertas em suportes de armazenamento digital.

É descrita como a utilização de várias técnicas de análise e investigação para identificar, recolher, examinar e preservar algum tipo de informação digital, sendo que tem como objectivo descobrir provas de determinado tipo de actividade e reportar essas provas, para que finalmente, possam ser utilizadas para fins, judiciais, para explicar o estado actual de determinada prova digital.

Essa informação digital pode ser proveniente de vários meios como discos rígidos, dispositivos USB, PDA's, telemóveis, CD's e DVD's, etc.

Metodologia:

1. **Análise do incidente (entendimento do cenário ou circunstâncias)**
2. **Recolha das provas**
3. **Análise das provas**
4. **Preparação de relatórios e conclusões**
5. **Glossário técnico resumido**

Prioridades de informática forense

- **Metodologia acima da tecnologia**
  - Investigar/analisar o crime e não a tecnologia
  - Documentar tudo
- **Reavaliação constante das provas**
  - Confirmar resultados com várias ferramentas forenses se necessário
- **Prove-o!**
  - Reunir o máximo de evidências possíveis

Definição de Análise Forense

Costuma definir-se análise forense, na sua acepção mais ampla, como a "ciência aplicada a questões de interesse legal". No contexto das T.I. e da Segurança da Informação, define-se como "a inspecção sistemática e tecnológica de um sistema informático e dos seus conteúdos para a obtenção de evidências de um crime ou qualquer outro uso que seja investigado".

A análise forense é uma peça chave nos processos de resposta a incidentes de segurança e serve para estabelecer dados como o "quê", "quem", "quando", "como" e, em alguns casos, o "onde" e o "porquê" de um incidente.

Análise Forense

Análise Forense no mundo Empresarial

Em muitos casos é difícil aplicar as técnicas de investigação forense no mundo de uma grande empresa.
Isto pode dever-se a muitas causas:

•Tamanho do ambiente tecnológico, distribuição geográfica, grande número de sistemas, tamanho do armazenamento, etc.

•Complexidade tecnológica e existência de múltiplas tecnologias

•Complexidade organizativa, política ou legal, incluindo diferentes jurisdições ou sistemas legais

•Existência de sistemas críticos em ambientes controlados

Análise Forense

Análise Forense no mundo Empresarial

Coisas tão básicas como a distância, a possibilidade de acesso físico a sistemas remotos (talvez ao outro lado do mundo), diferenças culturais ou de idioma, zonas horárias, etc. podem limitar ou dificultar a realização de uma investigação forense.

Quando se tem que obter a evidência de forma remota, a largura de banda disponível (às vezes mínima) e a proliferação de grandes meios de armazenamento (discos de centenas de gigabytes), tornam difícil a obtenção de imagens de disco para exame.

A existência de sistemas de armazenamento externo (NAS, SAN, etc.) e a ténue separação por vezes existente entre o físico e o virtual (sistemas virtuais, armazenamento distribuído, clusters geográficos) só complicam ainda mais a tarefa do investigador. O tamanho dos volumes actuais de disco, no melhor dos casos, pode implicar várias horas para realizar uma imagem bit-a-bit, localmente, sendo no entanto um recurso em uso corrente e rotineiro através de laboratórios forenses portáteis.

Evidência Digital

A evidência digital não deixa de ser um tipo de evidência física, embora seja menos tangível. Ela é composta de campos magnéticos e pulsos electrónicos que podem ser recolhidos e analisados através de técnicas e ferramentas apropriadas possui algumas características próprias como:

• A possibilidade de ser duplicada com exactidão. Uma prática comum entre os Especialistas Forenses, pois assim examinam a cópia e evita-se danificar a evidência original;

• Permite verificar a sua integridade através de ferramentas apropriadas.

• Difícil de extinguir. Mesmo apagando-se um ficheiro ou formatando um disco ainda é possível recuperar as informações nele contidas.

• Por outro lado, a evidência digital é extremamente volátil, podendo ser facilmente alterada durante o processo de análise;

A necessidade de especialistas certificados

Quando se lida com suportes informáticos com fins periciais em sede processual depara-se com quatro tipos de problemas principais.

1. Como recuperar a informação dos suportes, preservando a integridade da prova.
2. Como armazenar e manusear de forma segura, dados recuperados.
3. Como localizar a informação relevante perante o volume de dados.
4. Como apresentar a informação em sede de relatório, e defendê-la de forma técnicamente inquestionável.

Obtenção evidência

Quando a evidência se compõe de listagens de centenas de ligações, dezenas de processos a correr e uma imagem "bit-a-bit" de umas centenas de gigabytes de disco rígido, é necessário estabelecer um plano para a forma de realizar a análise.

Isto é, decidir de antemão o que é importante, o que não é e em que ordem fazer as coisas, o que mais uma vez, nos leva ao conhecimento quase total por parte do especialista forense, dos factos e objectivos da intervenção.

Obtenção evidência

Como regra geral, deve obter-se a evidência da forma menos destrutiva possível e sempre na ordem do mais volátil para o menos volátil, na ordem que se mostra a seguir:

1. Conteúdo da memória
2. Ligações de rede estabelecidas
3. Processos a correr no sistema
4. Portas abertas
5. Utilizadores ligados ao sistema
6. Conteúdos de ficheiros de paginação e swap
7. Conteúdos de sistemas de ficheiros
8. Configuração de hardware e periféricos

Obtenção evidência

Desligar ou não desligar?

Um elemento da metodologia que é importante ter claro é a decisão de desligar ou não desligar a máquina e, no caso de não desligar, se se deve mantê-la ligada à rede ou não.

Toda a decisão que se toma desde o momento em que se inicia a investigação deve estar meditada, ponderada e avaliada em relação aos possíveis benefícios e possíveis prejuízos.

Nos casos onde a actividade maliciosa é clara e onde cada segundo que passa gera mais danos para a organização, pode ser boa prática desligar o cabo de alimentação (melhor que desligar usando a função "desligar/shutdown" do sistema, que tende a alterar mais o estado da evidência(inclusivamente time stamps)).

Naturalmente que, neste caso, temos que ter decidido que o conteúdo da memória não é importante ou já obtivemos anteriormente uma imagem da memória ou informação útil sobre os processos activos.

Há casos em que desligar um sistema da rede, particularmente servidores de aplicações críticas de negócio online, não é uma opção. Seja pelo impacto que pode ter no negócio ou por motivos reguladores ou de processos restritos de gestão de trocas, uma queda não planeada de um sistema crítico pode ser pior que a incidência que se está a investigar.

Recolha de evidências

Para uma prova digital ser validada, é necessário demonstrar que a mesma é válida e não foi previamente manipulada, porque as conclusões de um caso dependerão muito das provas. No que respeita a provas digitais, a preservação das mesmas de acordo com métodos específicos, é uma regra importante, porque uma das primeiras coisas que acontecerá é a tentativa de desacreditar as provas apresentadas.

Para todo o processo de investigação forense existem alguns actos que devem ser evitados, para que as provas digitais não sejam comprometidas. São eles:

- Não executar nenhum tipo de aplicação que possa alterar datas dos ficheiros;
- Não utilizar aplicações de clonagem / imagem convencionais;
- Não utilizar o disco rígido sem bloqueadores de escrita.

Recolha de evidências

Fotografar e efectuar um diagrama de ligações do suporte/computador e correspondentes cabos de ligação (croqui).

Etiquetar todos os conectores e cabos para permitir uma reconstituição mais tarde se necessário. Etiquetar portas de ligação não usadas como "não em uso". Identificar "docking stations" de portateis, pois podem conter outros dispositivos de armazenamento de dados.

Registar e anotar as evidências de acordo com o SOP
(Standard Operating Procedures-Boas Práticas)

Cadeia de custódia de prova

A cadeia de custódia de prova DEVE ser sempre assegurada. Deverá ser usado e preenchido formulário próprio a acompanhar sempre a evidência. Qualquer pessoa que manuseie a evidência, independentemente do tempo que esteja na sua posse, deverá assinar e preencher o formulário de cadeia custódia de prova.

A cadeia de custódia determina como se utilizaram as provas digitais e o seu armazenamento:

- Quem recolheu, quando recolheu e onde foram recolhidas as provas;
- Quem analisou, quando analisou e como se analisaram as provas;
- Quem teve posse e durante quanto tempo tivemos posse das provas;
- Quando e entre quem foram transmitidas as provas.

O método científico

A palavra método vem do grego μέθοδος (méthodos, caminho para chegar a um fim). O método científico é um conjunto de regras básicas para desenvolver uma experiência a fim de produzir novo conhecimento, bem como corrigir e integrar conhecimentos pré-existentes. Na maioria das disciplinas científicas consiste em juntar evidências observáveis, empíricas (ou seja, baseadas apenas na experiência) e mensuráveis e as analisar com o uso da lógica. Para muitos autores o método científico nada mais é do que a lógica aplicada à ciência.

Fonte : www.wikipédia.org

Aplicar o método cientifico à informática forense

1. Métodos imparciais
2. Resultados repetíveis
3. Documentação completa
4. Resultados confirmáveis
5. Criação de hipóteses
6. Clara, concisa e objectiva explicação dos resultados
7. Formulação de uma teoria

As orientações base da informática forense

1. Dispositivos de armazenamento de dados devem ser esterilizados em ambiente laboratorial forense.
2. Deve ser usado software licenciado.
3. Os procedimentos devem manter a integridade dos originais.
4. As potenciais provas devem ser devidamente marcadas, analisadas e controladas.
5. Não manusear erradamente as evidências
6. Não trabalhar no original
7. Não confiar nos S.O.`s dos equipamentos a analisar
8. Documentar TUDO

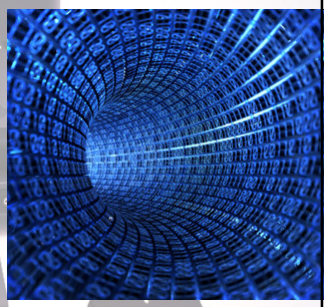
Documentar ("logar") tudo

1. Documentar todos os procedimentos em detalhe
2. Não confiar em "log´s" automatizados
3. Documentar de forma que qualquer pessoa, seguindo os mesmos passos, chegue às mesmas conclusões
4. Os log´s têm que coincidir com o SOP ("Standard Operating Procedure"- Boas práticas)
5. Confirmar sempre os resultados manualmente
6. Descrever os passos/acções e a metodologia utilizada.

Importância da Arquitectura

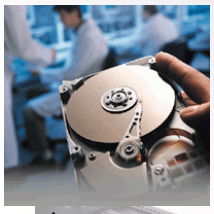
O trabalho pode ser dificultado caso a arquitectura de rede em que se encontra o/os equipamentos comprometido não estiver bem elaborada, como por exemplo, sem detectores de intrusão (IDS), sem logs do Firewall, sem logs do sistema.

Portanto, um bom trabalho futuro é elaborar uma arquitectura de rede que forneça, informações suficientes para garantir que se consiga encontrar o invasor e saber o que ocorreu no sistema comprometido de forma eficiente.



Cópia exacta de suporte(s)/informação

Copiar não é suficiente!



"Bit stream copy" (cópia bit a bit) inclui o backup de todas as áreas de um suporte informático.

Tais cópias replicam todos os sectores (bit a bit) do suporte, incluindo informação, metadata, áreas de sistema, "slack space" e "free space".

Criar, autenticar e preservar uma imagem "bit stream"

- Ferramentas credênciadas
- Utiliza-se sempre hardware "read-only" (bloqueadores físicos de escrita)
- MD5 Hash da imagem (certificação de autenticação)
- Triage-ID
- WinHex
- MD5 Summer
- Encase
- FTK
- …

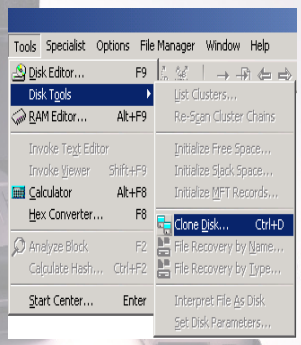
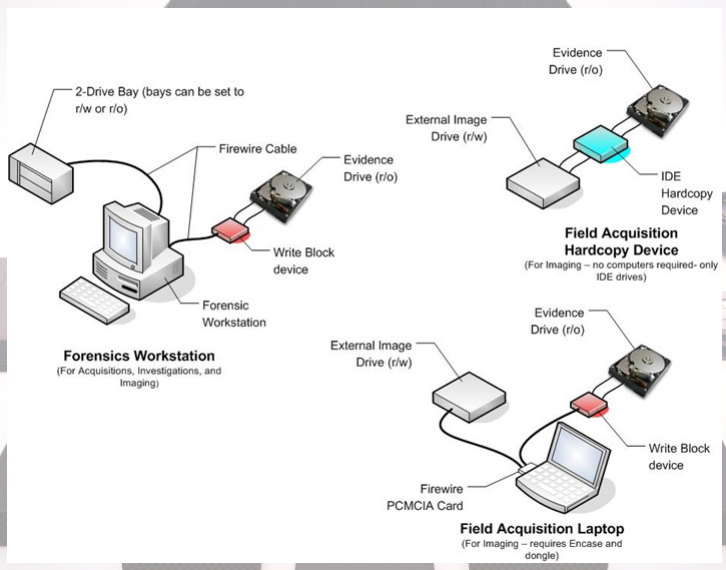


Diagrama de equipamentos de laboratório forense



Prova digital

O que distingue evidências digitais das tradicionais evidências em suporte de papel na análise forense e consequente investigação criminal ?

- Ficheiros electrónicos que se presumiam destruídos/apagados, podem vir a ser recuperados.
- Valiosa informação como datas, horas, nomes de autores podem estar embutidos na versão electrónica do documento/ficheiro.

Prova digital

- Evidências e provas digitais encontram-se espalhadas sob várias apresentações, formas e localizações num sistema informático. A "chave" para encontrar esta informação reside em compreender os tipos de informação que possa existir para procurar por cada tipo.

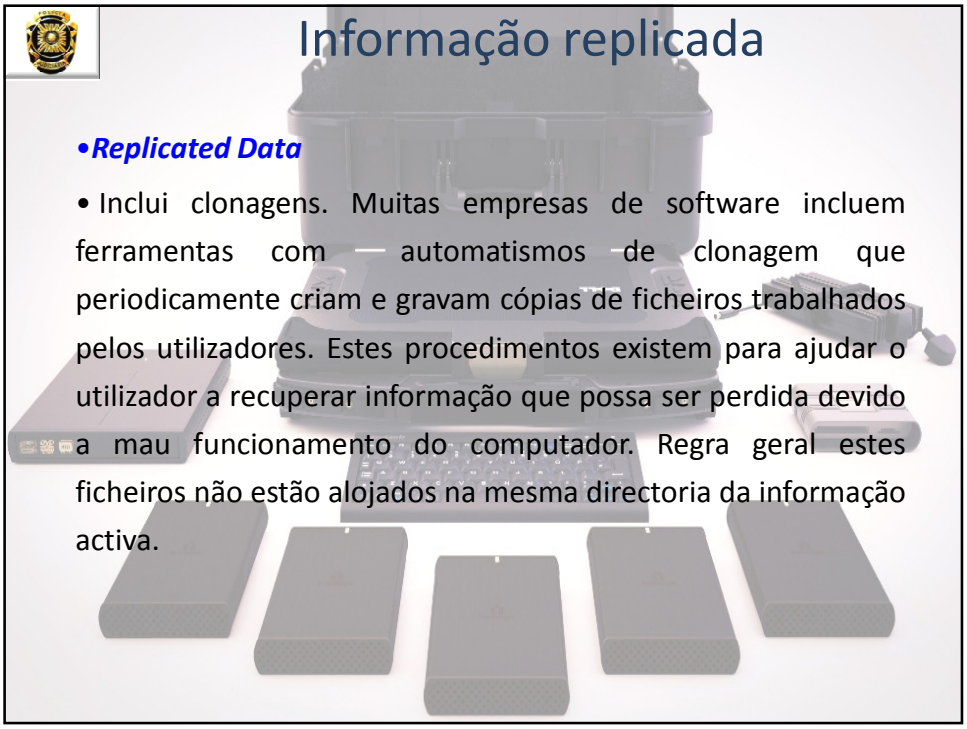
- Ficheiros de informação:

Informação processada e guardada electrónicamente pode ser dividida em quatro (4) categorias:

Informação activa

- ***Active Data:***
- É a informação legível, disponível e acessivel aos utilizadores.
- Inclui documentos de word, folhas de cálculo, bases de dados, processadores de texto, correio electrónico, agendas, contactos, etc.

Informação replicada



- ***Replicated Data***
- Inclui clonagens. Muitas empresas de software incluem ferramentas com automatismos de clonagem que periodicamente criam e gravam cópias de ficheiros trabalhados pelos utilizadores. Estes procedimentos existem para ajudar o utilizador a recuperar informação que possa ser perdida devido a mau funcionamento do computador. Regra geral estes ficheiros não estão alojados na mesma directoria da informação activa.

Informação de Backup

- ***Backup Data***

- É a informação copiada para suportes autónomos e amoviveis para possibilitar o restauro da informação no caso de uma falha do sistema. Os servidores são normalmente sujeitos a backup´s de rotina enquanto que os utilizadores, numa base informal não.

Informação residual

- ***Residual Data***

- É informação que se presume perdida/destruída mas ainda é recuperável do sistema informático. Inclui ficheiros "apagados" ainda existentes no disco rígido e informação existente noutro hardware do sistema como as memórias "ram", das impressoras (buffer´s), fotocopiadoras, faxes, etc.

Informação residente na memória de buffer é, regra geral, limitada a recentemente criada e guardada apenas.

Informação residual

Free Space

Quando um ficheiro é apagado, a informação não é "limpa".

Apenas o sistema marca o espaço do ficheiro como "livre". Referências ao ficheiro "apagado" são removidas das listas das directorías (raíz ou sub-directorias), mas os bit´s e bytes que constroem o ficheiro, mantêm-se no disco rígido até serem "overwritten" por nova informação.

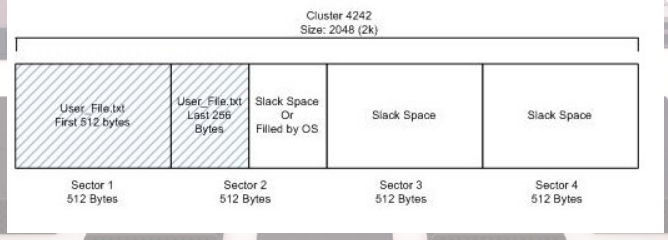
Slack Space

O "Slack space" é criado porque o S.O. do suporte apenas guarda informação na proporção de um ficheiro por cada cluster.

A percentagem do cluster não usada pelo ficheiro, define-se como "file slack". Se se reescrever um ficheiro apagado com um outro e este for de menor tamanho, ainda restarão fragmentos de informação no "slack space".

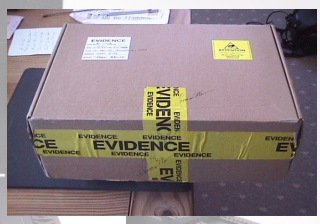
Slack Space – Definição ilustrada

Como ilustrado infra, guardar um ficheiro de 768 bytes (chamado User_File.txt) exige apenas o sector 1 e 1 / 2 do sector 2 no cluster. Dependendo do SO, os restantes 256 bytes no sector 2 podem ser preenchidos com 1's ou 0's ou pode simplesmente permanecem intactos. Ambos os sectores 3 e 4 não seriam escritos, sendo assim considerado Slack Space. Se o Slack Space anteriormente continha dados de um ficheiro eliminado, esta informação pode ser recuperada com ferramentas forenses.



Análise das Provas Digitais

Para a análise das provas digitais existem alguns procedimentos a seguir que dependem muito do tipo de cenário que foi desenhado anteriormente ou do tipo de provas que se procura. Algumas das análises que poderão ser efectuadas são :

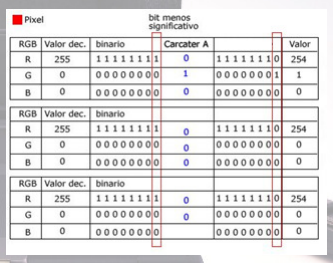


- Definição de uma linha temporal;
- Análise de palavras-chave;
- Análise de header´s de ficheiros;
- Análise de valores Hash;
- Análise de informação escondida ou apagada;
- Análise de Malware (ex. rootkit, cavalo de Tróia, spyware, etc.)
- Análise de processos;
- Análise de Log´s;
- Análise do registo de sistema;
- Esteganografia;
- Análise de correio electrónico (sempre com o total cumprimento dos pressupostos legais);
- Análise de páginas Web;
-Análise da modificação de informação;
-Criptografia
-Reverse Engineering
- Entre outros.

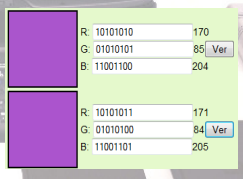
Esteganografia

Ex. Formatos:

- Textos;
  - . Deslocação de linhas verticais
  - . Deslocação de palavras ou textos justificados
  - . Deslocação do caracter de fim de linha
- Imagens;
  - . LSB
  - . Máscara e filtragem
  - . Algoritmo e transformação
  - . Spread spectrum
- Audio;
  - . LSB
  - . Parity Coding
  - . Phase Coding
  - . Spread spectrum
  - . Echo Hiding
- Video;
  - .Similar às imagens porque guarda nos frames do video
- Pacotes TCP/IP
  - . Campos não utilizados no header do pacote
  - . Alteração do número sequencial do pacote (ISN)



Camuflagem LSB



Hardware forense

- Suporta todo o tipo de ligações, média,etc.
- Tem "Write Protection"- Built in
- Memoria e velocidade do disco são dois dos mais relevantes aspectos.
- Depois de efectuada a imagem forense, index e "hashing" são procedimentos mais céleres em discos mais rápidos e máquinas com mais memoria.
- Tempo médio de vida, regra geral curto.

Hardware forense

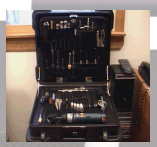
F.R.E.D. - Forensic Recovery of Evidence Device

F.R.E.D.D. I.E, Roadmaster

Periféricos de Hardware

DriveLock

Sacos Antiestáticos



Caixa de ferramentas

Máquina Fotográfica, luvas, gravador audio, etc

Sistemas Anti-Forense

Tem-se constatado nos últimos tempos a existência cada vez mais preocupante de ferramentas que procuram impedir ou dificultar a actividade forense.

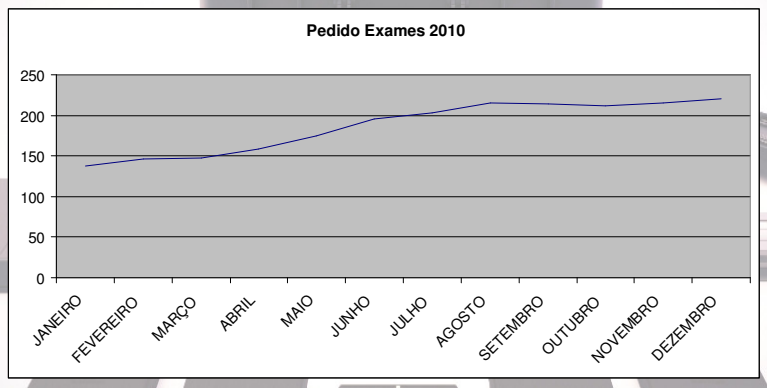
A ideia pode resumir-se na seguinte frase: **"Torna difícil que te encontrem e, se te encontrarem, torna impossível que o possam provar".**

Estas ferramentas existiram sempre de uma forma ou outra. A diferença é que agora são mais fáceis de encontrar por utilizadores não técnicos, como já sucede com as ferramentas de "hacking" que não requerem grandes conhecimentos técnicos para serem utilizadas.

Existem ferramentas que alteram os atributos da data (criação, acesso e modificação) dos arquivos de um sistema de arquivos, tornando impossível a análise clássica de sequência temporal.

Outras ferramentas permitem ocultar informação em partes não assignadas ao sistema de arquivos ou camufladas noutros ficheiros (imagens, som, etc.) E certamente, a existência de sistemas criptográficos de alta qualidade e facilidade de uso, dificulta mais ainda a obtenção de evidências no decurso de uma investigação, vindo as ferramentas forenses, mais uma vez, a desempenhar um papel crucial.

Estatística



Conclusões

O futuro da prática de investigação forense em sistemas informáticos passa necessariamente por renovar-se e incorporar técnicas amadurecidas que enfrentem:

A transferência do campo de batalha do disco duro para a memória. Certas aplicações, troianos e "rootkits" são capazes de residir em memória sem tocar no disco. A análise da memória e as ferramentas necessárias estão actualmente numa fase muito adiantada, ainda que haja algo promissor.

O desenvolvimento e aquisição de técnicas e ferramentas para a análise de dispositivos móveis e não móveis.

A entrada da prática forense no mundo Empresarial (sistemas críticos, grandes armazenamentos, falta de acesso físico a máquinas, virtualização, distâncias geográficas, cloud, etc.)

A proliferação e facilidade de obtenção, por parte do grande público, de ferramentas que dificultem a investigação forense.

Disponibilização de meios, técnicas, ferramentas e fundamentalmente FORMAÇÃO e CREDENCIAÇÃO adequadas.

Questões

ISCAC Instituto Superior de Contabilidade e Administração de Coimbra

Contactos:

Ricardo Amaral

Telef: 218641769

Email: ricardo.amaral@pj.pt

URL: www.pj.pt

Obrigado pela vossa atenção

"Na área Forense Digital, a excelência não é uma opção, é uma necessidade operacional." ***Anónimo in Internet***