Trabalho Prático

Análise Forenses Digital

António Pinto
apinto@estg.ipp.pt

Novembro 2022

1 Considerações gerais

O trabalho prático consiste na elaboração de um padrão (ou *pattern*) para a ferramenta ImHex (disponível em: `https://imhex.werwolv.net/`). O trabalho deverá ser desenvolvido em grupo. Serão aceites trabalhos individuais, desde que o aluno manifeste atempadamente a intenção de o fazer.

A deteção de trabalhos fraudulentos invalida a nota de todos os grupos de todos os trabalhos envolvidos. Serão considerados trabalhos fraudulentos, aqueles onde se verifique trabalho desenvolvidos por pessoas que não façam parte do grupo, na totalidade do trabalho ou apenas em parte deste.

1.1 Defesa

Todos os trabalhos práticos estão sujeitos a defesa por parte do grupo que o elaborou. A defesa decorrerá nas aulas práticas seguintes à data de entrega. A não comparência de um aluno à defesa implica a não consideração do trabalho para a nota do aluno em questão.

Uma defesa considerada como não satisfatória por parte do docente da disciplina implica a não consideração do trabalho para a nota do aluno em questão.

1.2 Outras considerações

Quando não seja respeitado o formato de entrega (tipos de ficheiros e nomes), os alunos que compõem o grupo sofrerão uma penalização de 10% na nota final do trabalho.

2 Datas

A data limite para **definição do grupo é 5 de dezembro de 2022, pelas 23h55**. A indicação da composição do grupo será efetuada pelo *moodle* (até um **máximo de 2 elementos**).

Após a definição de grupo, cada grupo deve enviar uma manifestação, por email, sobre qual o tipo de ficheiro que pretende analisar e elaborar o *pattern* para o **ImHex**. Não serão aceites formatos de ficheiros repetidos, sendo os mesmos atribuídos por ordem de chegada dos pedidos.

A data limite para a **entrega é 30 de dezembro de 2022, pelas 23h55**. Os trabalhos entregues fora de prazo não serão considerados. A entrega deverá ser efetuada por envio pelo *moodle*. Deverá ser entregue o *pattern* e o relatório num ficheiro ZIP com o nome: grupoX.zip (onde X deverá ser substituído pelo numero do grupo).

3 Padrões de tipos de ficheiros

A generalidade dos ficheiros de dados adota uma estrutura que pode ser analisada. Ferramentas como editores hexadecimais, o comando file, entre outras, processam os cabeçalhos dos tipos de documentos mais comuns e apresentam informação sobre estes. A listagem seguinte demonstra como obter alguma informação de um ficheiro JPEG recorrendo ao comando **file**.

```
aap@~ $file WinHex.png
WinHex.png: PNG image data, 1129 x 593, 8-bit/color RGBA, non-
    interlaced
```

A ferramenta ImHex (disponível em `https://imhex.werwolv.net/`) é um editor hexadecimal que possibilita a análise de padrões de ficheiros. A expansão dos formatos de ficheiros suportados é feita pela adição de ficheiros de configuração chamados de *patterns*. Os *patterns* já disponíveis para a aplicação podem ser acedidos pelo endereço: `https://github.com/WerWolv/ImHex-Patterns`.

Não poderão ser escolhidos tipos de ficheiros que já constem do repositório ImHex-Patterns.

Informação complementar pode ser encontrada em: `https://github.com/corkami/pics`

3.1 Relatório

O relatório a submeter deverá ser detalhado e incluir pelo menos a seguinte informação:

- Identificação e descrição dos tipos de ficheiros trabalhados, incluindo a descrição da sua estrutura.
- Descrição e demonstração dos *patterns* desenvolvidos.
- Confirmação, com recurso a ferramentas terceiras, dos resultados obtidos com os *patterns* desenvolvidos.

O único formato aceite para o **relatório é o formato PDF!**