# *Capture The Flag*: Método de Aprendizado para a Disciplina de Forense Computacional em uma Universidade Pública

**Carlos Eduardo B. Santos Júnior[1], Ana Clara N. Mendes[1], Jhonattan C. B. Cabral[1], Juliana B. dos Santos[1], Erick de O. Silva[1], Pedro H. R.Emerick[1]**

[1]Instituto Metrópole Digital (IMD)
Universidade Federal do Rio Grande do Norte (UFRN)
Caixa Postal 1524 – 59.072-970 – Natal – RN – Brasil

{ceduardobsantos, aclaranobre, cabral.jhon00
jubsbarbosa0, erickoliveira.eos, p.emerick98}@gmail.com

***Abstract.*** *Effectively evaluating the assimilation of content passed in the classroom is not always a trivial task. Therefore, new strategies are explored to ensure a better teaching experience. One of them may be the Capture The Flag (CTF), is a competition focused on solving information security challenges and that can approach issues related to computer forensics. This study aims to use the competition to measure the knowledge acquired through the discipline of Computational Forensics offered by a public university.*

## 1. Introdução

A utilização da internet se tornou intrínseca na sociedade atual, por exemplo, muitas pessoas utilizam alguma ferramenta para troca de mensagens instantâneas, transações bancárias, comércio eletrônico, e etc [Tanenbaum and Wetherall 2011]. Sendo assim, deve existir mecanismos para assegurar que os dados usados nos serviços estejam seguros.

Para introduzir e trabalhar os conceitos ligados à área da Segurança da Informação, foi ofertada por uma Universidade Pública a disciplina de Forense Computacional, uma das áreas da ciência forense que está em constante crescimento [Garfinkel 2010]. Durante as aulas, surgiu a necessidade de saber se os conhecimentos estavam sendo assimilados de forma correta, decidiu-se então aplicar desafios com situações que exigissem dos participantes os conhecimentos previamente apresentados durante as aulas. Por isso, foi pensado em produzir uma competição no modelo ”capture a bandeira”ou CTF, do inglês *Capture The Flag*. Nesse aspecto que este artigo foi escrito.

## 2. Forense Computacional

O avanço da tecnologia não trouxe apenas benefícios para a sociedade, trouxe também o aprimoramento de algumas práticas criminosas e o surgimento de outras. [da Silva Eleutério and Machado 2011]. Para apoiar o combate a estas práticas que surge a computação forense com o objetivo de determinar a dinâmica, mirando os esforços na identificação e no processamento de evidências digitais em provas materiais de crime [da Silva Eleutério and Machado 2011].

A resolutividade de práticas criminosas envolvendo dispositivos computacionais pode requerer uma análise minuciosa dos equipamentos responsáveis pelo armazenamento dos dados, em sistemas de arquivos com propriedades de aglomeração de dados consideravelmente boas, arquivos excluídos podem permanecer intactos durante

anos. Ou seja, informação de um arquivo excluído são como um fóssil: um esqueleto pode não ter a ossada completa, mas o fóssil permanece, imutável, até ser destruído [Farmer and Venema 2008].

## 3. Capture The Flag

No âmbito da tecnologia da informação, competições de CTF envolvem diferentes habilidades dos jogadores para resolução de desafios de segurança da informação. Segundo [Magalhaes et al. 2017], uma competição pode levar até vários dias e as equipes devem concluir o máximo de desafios de segurança cibernética que puderem.

No meio acadêmico e profissional muitas instituições têm promovido competições com este tipo de abordagem, a fim de melhorar os conhecimentos em cibersegurança e apoiar no aumento de profissionais nessa área [Matias et al. 2017]. Ademais, o CTF foi escolhido como uma maneira de mensurar o aprendizado da turma de Forense Computacional, pois como concluído por [McDaniel et al. 2016], esta metodologia proporciona a oportunidade dos alunos terem contato com a perícia forense similar ao mundo real.

## 4. Metodologia

O estudo foi realizado utilizando uma amostragem de 12 alunos efetivamente matriculados na disciplina de computação forense. Com desafios acessíveis por um período de 7 dias e para tentar soluciona-los, além dos usuários terem que se cadastrar na plataforma utilizada, teriam que estar em sala de aula. Após o estudo esperava-se que grande parte dos participantes demonstrassem um bom desempenho, o que seria caracterizado pela resolução de pelo menos metade dos desafios impostos.

### 4.1. Plataforma CTF

A plataforma utilizada foi a do grupo CTFd[1]. O uso desta plataforma nos permite analisar os dados de cada jogador, assim como do grupo de participantes, nos entregando informações, como submissões, quantidade de acertos e erros por desafio. A análise destes dados é que ao fim compõe nossas conclusões diante da absorção do conteúdo ministrado na disciplina.

### 4.2. Desafios da competição

Como o tempo de execução limitado, foram estabelecidos um total de 6 desafios para que fosse possível a realização de um desafio diariamente com mais um dia extra.

Um ponto importante a se destacar, é que o número máximo de usuários em um desafio foi de apenas 9, dado que foi divulgado o CTF como uma atividade avaliativa para uma disciplina de 19 alunos oficialmente matriculados. Um número considerado pequeno, representando aproximadamente 47% dos alunos, isto para o melhor caso apresentado, mostrando a falta de interesse pela maior parte da turma em aplicar as técnicas assimiladas.

No primeiro desafio foi fornecido um arquivo de *log* possuindo 3550 linhas. Na linha 239, foi inserido a *flag*. Os jogadores tinham como objetivo filtrar o conteúdo do *log* em busca da *string* F0RS3NS3, identificar o método de codificação utilizado para

[1]Disponível em https://ctfd.io/

esconder o texto original e, por fim, decodificá-lo. No desafio seguinte, ”Bela Imagem”, foi decidido avaliar a percepção e os conhecimentos de esteganografia dos alunos. Neste caso, uma mensagem foi ocultada em um arquivo com extensão (.jpg).

Para o terceiro desafio, ”Help!”, foi lançado uma história fictícia de uma situação de emergência em que os protagonistas possuíam apenas uma forma de se salvar. Foi entregue uma saída simples com o código morse. Neste caso, descobrir a *flag* era o menor dos objetivos, pois a identificação do tipo de codificação utilizada era a informação mais relevante do desafio. No desafio ”Periciando”, o quarto, o objetivo foi apresentar o que seria uma *flag* aos jogadores. Fornecendo um arquivo com extensão (.pdf) em que o conteúdo não se adéquava ao formato indicado pela extensão. Por fim, executando o arquivo com um software adequado para a extensão correta, o jogador teria um contato direto com a *flag* utilizada.

No desafio ”Pendrive suspeito”, se trouxe um ambiente próximo ao real fornecido um disco particionado do tipo ext3. Em seguida, os participantes deveriam converter o disco para o formato (.vdi) e inicializá-lo em uma máquina virtual. Os competidores ao acessarem o disco, analisariam e procurariam por arquivos deletados, mas que ainda possuíam *inodes*[2] alocados.

Similar ao desafio anterior, ”Quem é Ká?”, trouxe uma resolução com algumas etapas forenses para recuperação de um arquivo apagado. Entretanto, o tipo de partição do disco estava em FAT, com setor de *boot* DOS/MBR. Após a identificação, os arquivos deveriam ser restaurado para análise sendo possível descobrir o nome verdadeiro de ”Ka”.

## 5. Resultados

A primeira análise executada foi a relação entre a quantidade de tentativas para encontrar a resposta correta e os acertos. Pôde-se notar na figura 1 que o desafio ao qual foi realizado a maior quantidade de tentativas para se obter a resposta correta foi o ”Help !”, contrariando o que era esperado, uma vez que se tratava de um desafio simples e que não envolvia nenhum conhecimento profundo de análise forense, apenas o conceito de Código Morse.

Em contra partida, o desafio ”Pendrive Suspeito”que requeria um conhecimento mais avançado em análise de disco e sistemas de arquivos foi um que teve menos erros. Sendo assim, os alunos que conseguiam executar a sequência de passos chegariam na resposta sem uma quantidade elevada de tentativas.

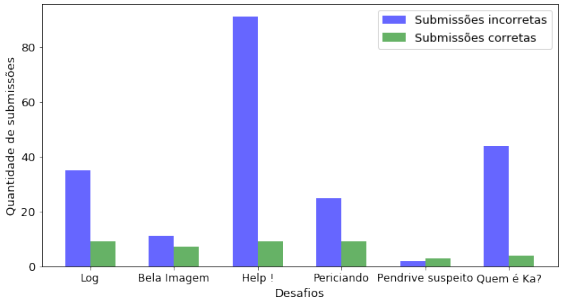


**Figura 1. Total de submissões por desafio**

[2]Tratam-se de estruturas responsáveis por conter informações básicas sobre arquivos e pastas.

O desafio ”Help!”, teve o maior número de respostas, ou seja, maior participação dos alunos (9 no total). Isto se deve à este desafio ser o mais simples dentre todos. No desafio ”Periciando”foi obtido uma menor adesão por parte dos alunos, o que foi inesperado já que o arquivo fornecido tinha como extensão (.pdf) e na realidade era uma imagem. Ao identificar isto, a *flag*, estava de fácil acesso.

O desafio ”Quem é Ka?”era semelhante ao do desafio ”Pendrive Suspeito”, o que consequentemente fez com que os resultados fossem semelhantes: número alto de submissões incorretas e pouca adesão dos alunos. Já no desafio ”Pendrive Suspeito”, houve poucas tentativas e pouca adesão dos alunos, pois se tratava de um desafio mais difícil e com mais etapas para obter êxito. Porém, considerando que as metodologias para realização da análise forense de dispositivos suspeitos foram vistas em sala de aula, era esperado que mais alunos conseguissem realizar o desafio.

## 6. Conclusão

O maior objetivo em utilizar uma competição do tipo CTF para avaliar os conhecimentos da turma de Forense Computacional é observar, principalmente, a postura do analista forense diante de investigações, que podem ser estressantes e necessitarem de diferentes tipos de conhecimentos, dependendo do tipo de perícia que se precisa realizar. Assim, foi observado que, apesar dos alunos terem absorvido bastante conteúdo oferecidos pela disciplina, a maioria não conseguiu sair da ”zona de conforto”em relação a execução dos desafios. Os alunos que obtiveram êxito para concluir os desafios alcançaram melhores resultados no final da disciplina.

## Referências


da Silva Eleutério, P. and Machado, M. (2011). *Desvendando a Computação Forense*. NOVATEC.

Farmer, D. and Venema, W. (2008). *Perícia forense computacional: teoria e prática aplicada : como investigar e esclarecer ocorrências no mundo cibernético*. PRENTICE HALL BRASIL.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Elsevier Ltd*.

Magalhaes, L., Antonio Carlos F. Petri, Gabriel de S. Alves, C. A. C. M., and Matias, P. (2017). Provisionamento automatizado de servidores para competições de segurança da informação. *XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg 2017*.

Matias, P., Barbosa, P., Cardoso, T., Mariano, D., and Aranha, D. (2017). Nizkctf: A noninteractive zero-knowledge capture the flag platform. `https://arxiv.org/abs/1708.05844`.

McDaniel, L., Talvi, E., and Hay, B. (2016). Capture the flag as cyber security introduction. *49th Hawaii International Conference on System Sciences*.

Tanenbaum, A. S. and Wetherall, D. J. (2011). *Redes de Computadores*. Pearson Prentice Hall, 5 edition.