The Forensic Challenger

Conference Paper · December 2014

DOI: 10.1109/ICWOAL.2014.7009231

1 author:

Alaeddin Alawawdeh
Norwegian University of Science and Technology
5 PUBLICATIONS **6** CITATIONS

SEE PROFILE

The Forensic Challenger

Øyvind Nordhaug[1], Ali Shariq Imran[2], Alaeddin M.H. Alawawdeh[1] and Stewart James Kowalski[1]
[1]*Dept. of Information Security,* [2]*Dept. of Computer Science & Media Technology,*
Gjøvik University College, Gjøvik, Norway
{*oyvind.nordhaug, alishariqimran, alaeddin.a*}*@gmail.com*

***Abstract*—This paper proposes a game based e-Learning tool called The Forensic Challenger (TFC) to teach digital forensic investigation. By combining elements from game theory with the use of e-Learning, the authors are able to provide a solution that offers a more efficient way of learning how to perform digital forensics investigations. Contrary to traditional learning methods, TFC is built on a Hyper Interactive Presenter (HIP) platform that incorporates VARK learning style model to take into account individuals' learning preferences. For visual and audio learners, it provides a video playback and Powerpoint presentation. Learners who prefer to read, there is a custom designed wiki page containing information relevant to the presented topic. While for kinesthetic learners, a multiple choice question based quiz is implemented, and a pedagogical chatbot agent is there to assist users. It provides easy navigation and interaction within the content. Preliminary results of the subjective experiment to evaluate the effectiveness of TFC suggests that such a system will prove useful in teaching digital forensic investigation to young students.**

***Keywords*-forensic challenger, eLearning, hyper interactive presenter, VARK**

I. Introduction

Performing a digital forensic investigation has become more complex as society is more dependent on computers. This creates a gap between the societys capability to investigate the crime, and the criminals likelihood to be caught and convicted. Digital forensics integrates the fields of computer science and law to investigate crime. For any digital evidence to be used in court, investigators must follow a proper set of procedures when collecting and analyzing data from computer systems [1]. Many of these laws were written before the era of computer forensics, and are often outdated. The inability of law to keep pace with technological advancements may in the end limit the use of forensic evidence in court.

These investigations are conducted by following various steps to ensure that the process is properly handled. Proper collection and examination of evidence is critical to avoid corruption and to preserve the evidence. Failing to do this, the gathered data may lose its admissibility as evidence. Understanding what must be done, and how it should be done is essential in a digital forensics investigation. This knowledge would also be useful for not only law enforcement that performs the investigations, but judges, lawyers and prosecutors as well as corporations.

In a paper published by Pan Yin et.al."Game-based Forensics Course For First Year Students" [2], the authors have developed a forensics course using the Game-Based Learning (GLB) approach. This system has direct access to forensics tools, and evidence from a suspects machine. This digital forensics game focus on visualizations to illustrate fundamental concepts in computer forensics, as well as interactive lab-based investigation modules to allow the students to practice in gathering, preserving, analyzing and reporting digital evidence.

Gary C. Kessler published his paper "Online Education in Computer and Digital Forensics: A Case Study" [3]. In this study, Kessler describes some of the course design aspects of teaching computer forensics in an online environment. The Champlain College's online course in digital forensics are using a Learning Management System (LMS). The LMS is an asynchronous virtual classroom which provides communication tools, allowing online students to interact with each other on many levels.

n 2006 the Champlain College performed a study to determine if the learning objectives were met equally well in online and on-campus courses. With no significant difference between the two delivery modes, the average grade of the online sections were slightly higher.

In this project we combined the use of E-Learning with the hands-on experience you get from participating in laboratory sessions with a digital forensics investigator. We named the developed platform The Forensic Challenger (TFC). The platform uses the Hyper Interactive Presentation (HIP) platform as a test platform [4]. By using the HIP platform we combine the use of visual, auditory and kinesthetic learning. This investigation will go through a fictional scenario and the player has to answer a series of questions regarding this scenario. This satisfies on a very basic level the kinesthetic learning, as the user get to experience recordings of live examples. During this challenge, the user have the possibility of accessing a specifically crafted Wiki as well as presentation of the topics in video. The expected result of this method is increased learning performance and motivation for the students.

The Forensic Challengers novelty comes from being entirely web based, and it gives the users the ability to use their preferred medium i.e. video, powerpoint slides, wiki documents, chat bot etc., to learn from. This is plausible due to the fact that each component in HIP maps one component of VARK (visual, auditory, read/write and kinesthetic) learning [5] style model. Thereby, giving the possibility to the user to use the learning method adequate

978-1-4799-5739-2/14/$31.00

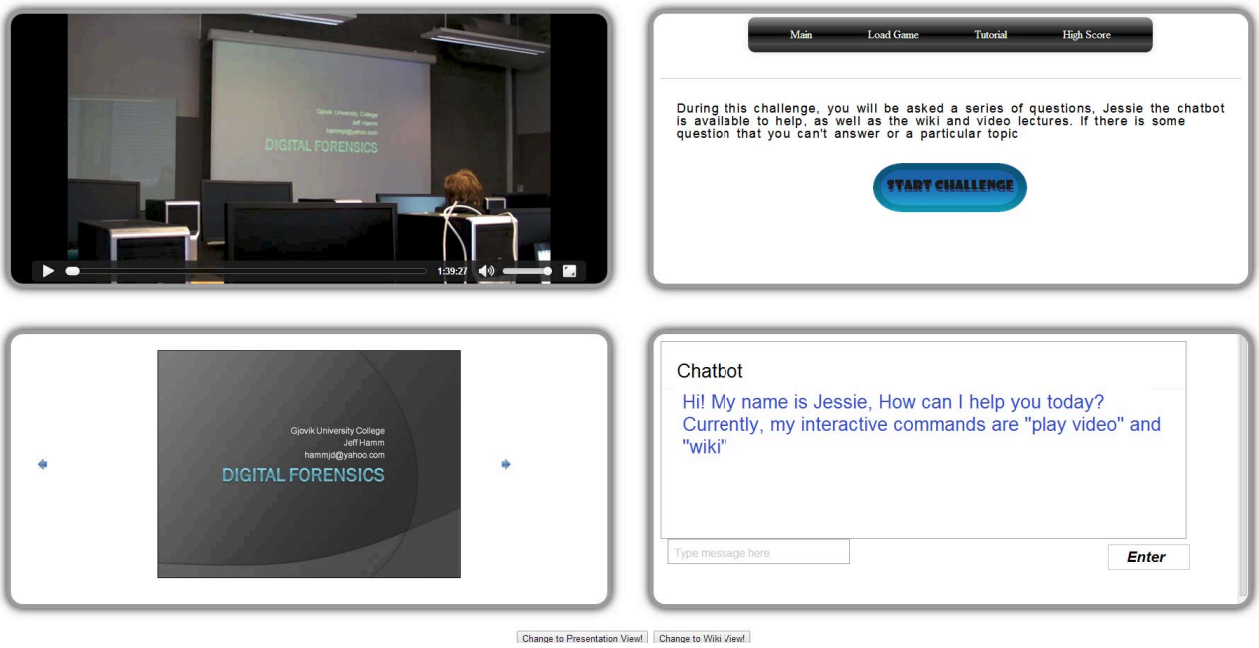

Figure 1. The Forensic Challenger Interface

for them depending on their learning needs.

The rest of the paper is organized as follows. Section 2 describes the proposed method in detail. In section 3 we describe the subjective experiment, while section 4 gives an analysis of the results. Lastly, section 5 concludes the paper.

II. The Forensic Challenger

The Forensic Challenger is hosted on a web server program called Apache and is built up using Django and the corresponding modification "mod-wsgi" to handle the interactions with Apache. The conversational agent back-end is a python module called PyAIML, which is based on the A.L.I.C.E project [6]. HyperText Markup Language (HTML5) and Cascaded Style Sheets (CSS3) as well as JavaScript handles the front-end of the platform. The Forensic Challenger interface can be seen in Figure 1, and consists of four components which are described in the following subsections:

A. Video and Presentation Playback

The Forensic challenger provides two visual tracks for the learners as a supporting material to learn from. One consist of a video lecture and the other contains images of Powerpoint presentation. They are designed keeping in mind the needs of the visual learners. In [7], Neil Flemming has identified four different kinds of learning styles i.e. visual, auditory, read/write and kinesthetic in the VARK model and has grouped individuals into one of these categories based on their learning preferences. Video and presentation playback component of TFC takes into account the first two aspects of the VARK model - visual and auditory.

TFC video and presentation playback is based on the core HIP functionality, which comes from the HTML5 property currentTime. The currentTime property sets or returns the current position (in seconds) of the audio/video playback. When the property is set, the playback will jump to the specified position. The platform is able to synchronize presentation slides with the video, or jump to a position of interest for easy navigation by using a list of timestamps containing the slides appearance information in the video and viceversa.

B. Wiki Page

To give the users access to information specifically for the challenge, we decided to create a knowledge database in form of a wiki. This wiki page was a open source wiki called "django-Wiki" designed specifically for Django. The framework was developed by Ben Jao Ming [8], with help from the development community. The wiki page was populated with the supplementary information corresponding to the challenges and the content presented in form of video and Powerpoint presentations. It takes into account the third aspect of the VARK model i.e. read/write, providing a medium for individuals who are textual learners.

C. Chatbot

The chatbot is implemented to be a pedagogical agent for the users, which is meant for discussions and help with the topics. It partially takes into account the kinesthetic aspect of VARK model and also acts as a navigation tool. The chatbot have the same functionality as the buttons in the challenge frame. You can tell it to "play video" and it will offer the same functionality as the Show video button, likewise with the wiki. Additionally you can say "I need help with (something)" and it will open the wiki and search for this specific keyword.

D. Challenger

The Forensic Challenger uses a frame which is reserved for the challenges. The purpose of these challenges is to test users knowledge about a given topic in investigating crime. It lets a user choose his/her answer and progress in the challenge they have chosen. From this frame they have the possibility of interacting directly with the other frames to seek knowledge from either the video recording or the wiki page. This is done by clicking a button, which will take them to the exact position in the video and the Powerpoint presentation where the topic is presented. Challenger uses an out of the box CSS3 navigation bar to traverse between the different challenges, look at tutorials or high-scores. Challenger satisfies the kinesthetic aspect of VARK model where people learn by doing the challenge.

TFC employs a simple, robust and primitive solution for a challenge frame instead of the character progression system. The score system that has been implemented is one of these features. After the challenge is complete, the game gives users the results of their answers in points. The questions answered will be either true or false, but the challenger will not show what the right answer is. This is intentional, as it encourages the user to spend more time finding the correct answer.

The challenge itself is started after a brief introduction to the challenge, by clicking the "Start Challenge" button. In case of the user has already completed the challenge, the next challenge can be loaded from the menu. The questions in this challenge have all the same format as shown in Figure 2, a multiple choice question with varying number of answers. There are a few questions that show a picture which relate to the question, that will be shown below the question.

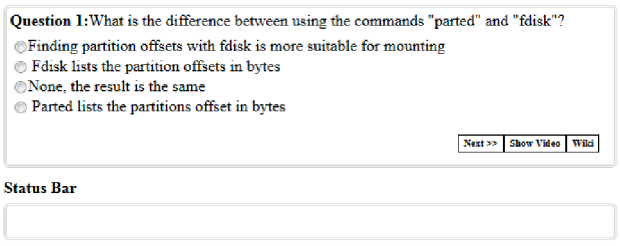

Figure 2. Example of a Challenger question

In this example, the challenge gives the user a choice between 4 answers, if the user knows the answer, he can select his choice and click "Next". If the user wish to watch the specific position in the video where this is mentioned, he can click the "Show Video" button, and the video and presentation slides (if any) is loaded in the other frames at the correct position. If he desires to read on the wiki page, he will click the "Wiki" button, and the wiki page is loaded at the correct topic. When the user is comfortable with answering the question, he can select his choice and click next, and the next question is loaded. The progress bar will keep track of how many questions are answered in the challenge.

After answering the last question, the user will get a score, each question is equally weighted at 20 points per right answer, and 0 points for a wrong answer. Additionally, it will list what question were right or wrong, but not what the correct answer is.

III. Experiment Setup

This section briefly explains the experiment setup to test the effectiveness of TFC. TFC consists of video, wiki page, chatbot and challenger. These components are organized based on HIP platform presentation method. All these frames contain learning material about digital forensics. The experiment is divided into two groups. Both groups have the same learning materials. Group A have the powerpoint presentation slides and the video to learn from, while group B have the material presented in a TFC platform. A subjective experiment is conduction, comparing group A - *the Fronter group* to group B - *TFC group*. Fronter [9] is a learning management system being used at Gjøvik university college. Group A is the group which performed the experiment using only the provided raw material via Fronter, while group B got access to the TFC platform. The number of participants in group A is 27, while 24 persons participated in group B.

In this experiment we used a questionnaire for each group. The survey directed to the group A contain six questions. While the questionnaire directed to group B contain 9 questions. Some of these questions are based on a Likert scale like question 1, 5 and 6. Also there are similar questions for both of the groups, like question 1, 2, 3 and 4. The likert scale that we used in this experiment contain five items or response for each question. A five-level Likert scale is used where 1 corresponds to strongly disagree while 5 corresponds to strongly agree.

IV. Result and Analysis

This section presents the results of the survey questionnaire of participants from group A, those who used the Fronter to group B, who used TFC for the following questions:

a) On a scale from 0 to 5, how interested are you in digital forensics? Figures 3 and 4 show how interested the participants are in digital forensics. The results show that the answers are approximately similar for both groups, with a slightly higher interest in group B.

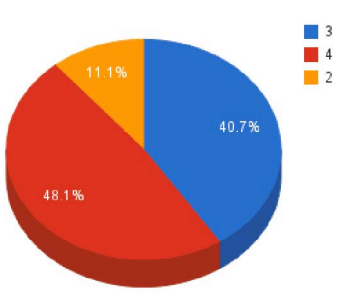

Figure 3. Question 1: Distribution with Likert scale for group A

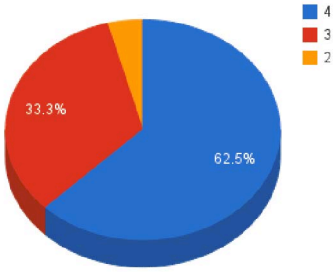

Figure 4. Question 1: Distribution with Likert scale for group B

b) Would you recommend The Forensic Challenger / File-share approach to a fellow student who is interested in digital forensics?

The results in figure 5 and 6 showed clearly that group A was not particularly satisfied with the solution of giving the students the raw video footage and presentation slides from the lab session. In group B, most of the participants answered that they would recommend TFC to a fellow student interested in digital forensics.

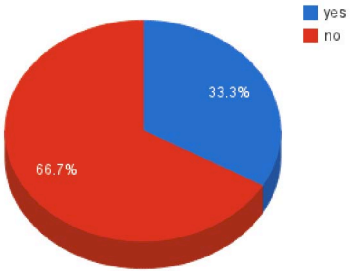

Figure 5. Question 2 for group A

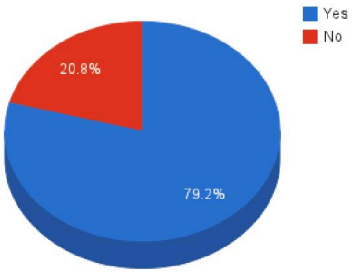

Figure 6. Question 2 for group B

c) How much time did you use to find all the answers in the challenge? In this question we tried to estimate the time consumption of locating the correct information. As shown in figure 7 and 8, group A spent a lot longer time to answer the same set of questions. Most of the participants in group A spent 30 to 40 minutes, while on the contrary most of group B spent less than 10 minutes. Since the motivation level of the two groups were almost identical, the result from this question shows that group B had a much easier time answering the questions.

d) Group A exclusive - How many questions were you able to complete? For group A we asked a question about

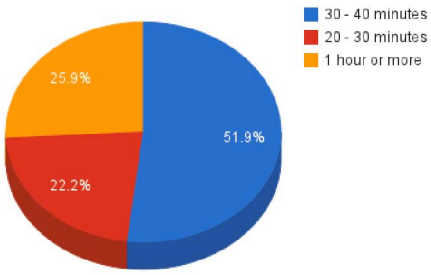

Figure 7. Question 3 for group A

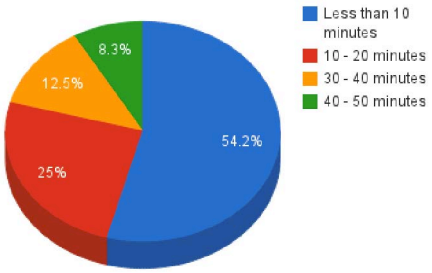

Figure 8. Question 3 for group B

how many questions they managed to complete. Although group A does not get any feedback whether the answers are correct or not. Completion of the questions mean that they had obtained enough information to be confident in their answer as shown in figure 9.

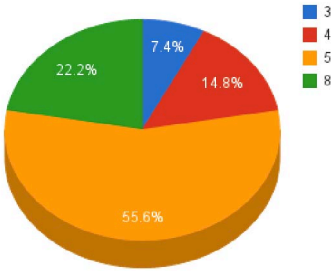

Figure 9. Question 4 for group A

e) Group B exclusive - How many of the answers did you find in the video recording? Question 4, 5 and 8 tried to establish what elements in the TFC platform were most useful. As shown in figure 10, for question 4, which is how many answers were found in the video recording, most participants selected 20 and 40 percent. This could have various reasons; the video recording itself was not very good, and the participants chose to look for information elsewhere. It could also mean that they are not visual learners and is subconsciously drawn to other types of information.

f) Group B exclusive - How many of the answers did you find in the wiki page? Figure 11 shows the results of question 4 for group B depicting the number of answers found in the wiki page is small. The reasons for this

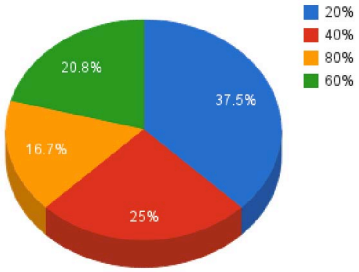

Figure 10. Question 4 for group B

could be the same as we discussed for the previous question. If these results are based on the learning style of the students or not is hard to determine without a learning style test.

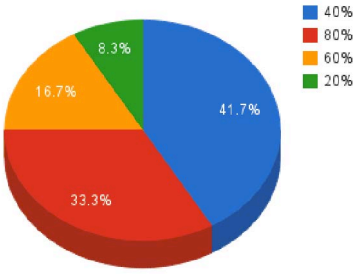

Figure 11. Question 5: Distribution with Likert scale for group B

g) Group B exclusive - On a scale from 0 to 5, did you find the chatbot useful? The usage of the chatbot was not expected to be high. It is in the latest version not very useful to begin with. As shown in figure 12, 45.8 % of the participants responded 1 to this question and 33.3% responded 0, which means that the chatbot was not useful for the most of the students.

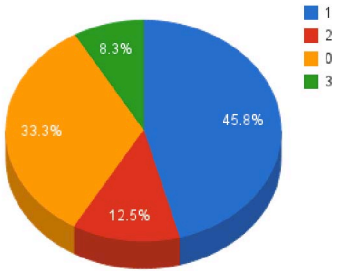

Figure 12. Question 8: Distribution with Likert scale for group B

h) On a scale from 0 to 5, how much did you learn from this challenge? The result of this question is of high value. The participants were asked how much they thought they learned from participating in the challenge, and the differences were quite obvious. As shown in figure 13, most of the participants in group A did not learn anything from the challenge except for some highly motivated participants. The highly motivated participants would learn something regardless of how the information is presented to them. With group B, the participants seemed to have learned more from doing the challenge as shown in figure 14.

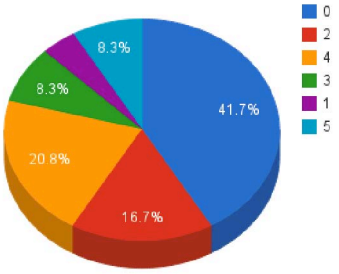

Figure 13. Question 5: Distribution with Likert scale for group A

i) On a scale from 0 to 5, how much would you like to participate in a similar challenge? Group A mostly did not wish to participate in a similar challenge as shown in figure 15, in contrary to group B where the interest was much higher as shown in figure 16.

V. Conclusion

This research proposes the use of game mechanics combined with VARK learning model in the Forensic Challenger tool for teaching digital forensic investigation. The main aim of this research was to evaluate the usefulness of TFC and users' learning experience. A secondary aim was to explore if there's any change in a learner's motivation and level of participation with learning digital forensics investigation via TFC. The experiment was conducted on two groups of students. Group A used a LMS called Fronter to present the learning material, while group B

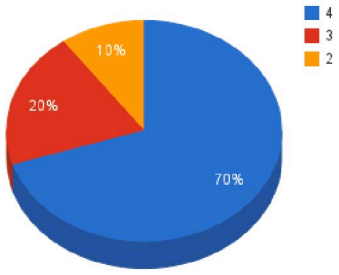

Figure 14. Question 6: Distribution with Likert scale for group B

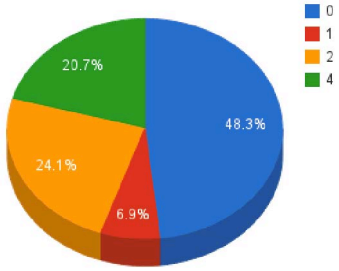

Figure 15. Question 6: Distribution with Likert scale for group A

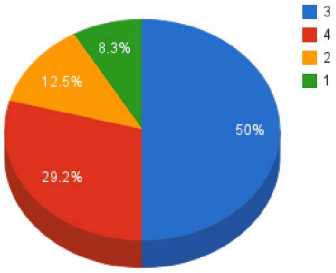

Figure 16. Question 9: Distribution with Likert scale for group B

used the TFC platform for their learning experience. The results indicate that the TFC had a positive impact on learning motivation levels. In the TFC group 79.2% would recommend the material to other students, while only 33.3% of Fronter group would recommend the material to other students. Also, the time used to find the answers in the challenge for the TFC group was much faster than Fronter group. We found that the interest level of students participating in similar challenge for TFC group was much higher than the Fronter group. The overall results concord the effectiveness of TFC in teaching digital forensic investigation.

REFERENCES

[1] National Institute of Standards and Technology (NIST), and United States of America. "Forensic Examination of Digital Evidence: A Guide for Law Enforcement." 2004.

[2] Pan Yin, Sumita Mishra, Bo Yuan, Bill Stackpole, and David Schwartz. "Game-based forensics course for first year students." In Proceedings of the 13th annual conference on Information technology education, pp. 13-18. ACM, 2012.

[3] Gary C. Kessler. "Online education in computer and digital forensics: A case study." In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on, pp. 264a-264a. IEEE, 2007.

[4] Ali Shariq Imran, and Stewart James Kowalski. "HIP-A Technology-Rich and Interactive Multimedia Pedagogical Platform." Learning and Collaboration Technologies. Designing and Developing Novel Learning Experiences. Springer International Publishing, 2014. 151-160.

[5] Uro Ocepek, Zoran Bosni, Irena Nanovska erbec, and Joe Rugelj. "Exploring the relation between learning style models and preferred multimedia types."Computers & Education 69: 343-355. 2013.

[6] A.L.I.C.E, Artificial Intelligence Foundation, http://www.alicebot.org, [Online], last accessed 15th September 2014.

[7] Neil D. Fleming. "I'm different; not dumb. Modes of presentation (VARK) in the tertiary classroom." In Research and Development in Higher Education, Proceedings of the 1995 Annual Conference of the Higher Education and Research Development Society of Australasia (HERDSA), HERDSA, vol. 18, pp. 308-313. 1995.

[8] Ben Jao Ming, Django Wiki, https://github.com/django-wiki/django-wiki, [Online], last accessed 15th September 2014.

[9] Fronter, https://fronter.com, [Online], last accessed 17th September 2014.