Ecole Publique d'Ingénieurs en 3 ans

Rapport

JEU SÉRIEUX FORENSIQUE

le 31 mars 2023,
version 2.0

BLAISE Florian,
ROUSSEAU Nicolas,
BRUANT Antonin,
PATRY Alan, BELMAHI Adib,
florian.blaise@ecole.ensicaen.fr,
nicolas.rousseau@ecole.ensicaen.fr,
antonin.bruant@ecole.ensicaen.fr,
alan.patry@ecole.ensicaen.fr,
adib.belmahi@ecole.ensicaen.fr

Tuteurs :
ROSENBERGER Christophe,
GIGUET Emmanuel,

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

www.ensicaen.fr

TABLE DES MATIÈRES

TABLE DES FIGURES

INTRODUCTION

1. Présentation générale du projet et du contexte

Nous avons été mandatés par le GREYC et Monsieur Rosenberger pour travailler sur un projet de jeu sérieux, avec pour thème la forensique. Ce jeu qui se veut ludique a pour objectif de faire découvrir le monde de l'investigation numérique à tout étudiant intéressé (collégien, lycéen, élève du supérieur), tout en prévoyant une courbe de difficulté pensée en conséquence.

Le projet, à terme, devra être accessible au public via la plateforme G'DIP et devra être déployable de manière événementielle (Fête de la science par exemple) afin de faire découvrir la forensique, ou d'en approfondir la connaissance.

Ce jeu s'articule autour d'un scénario découpé en plusieurs chapitres, qui permet aux participants de manipuler des outils de forensique (simulés par les créateurs du jeu) et d'apprendre les rudiments de ce domaine tout en s'amusant.

Le principe de notre jeu se rapproche d'un jeu de piste. Le but est, au travers de notre scénario, de suivre une histoire et de percer les mystères d'une clé USB égarée. Pour cela, le joueur va devoir répondre à une série d'énigmes pensées pour plaire au plus grand nombre.

2. Objectifs du projet

Design du gameplay :

- Créer un scénario
- Construire les énigmes qui vont composer le jeu, pour plusieurs niveaux de joueurs.
- Créer les fichiers-réponses aux énigmes.

Interface du jeu :

- Avoir une interface de jeu immersive pour guider les joueurs

Site d'application des filtres :

- Avoir un logiciel pouvant exploiter des bases de données afin de permettre au joueur d'appliquer des filtres sur des fichiers, et résoudre les énigmes.

CONTENU

3. Travail réalisé.

3.1. Schéma récapitulatif

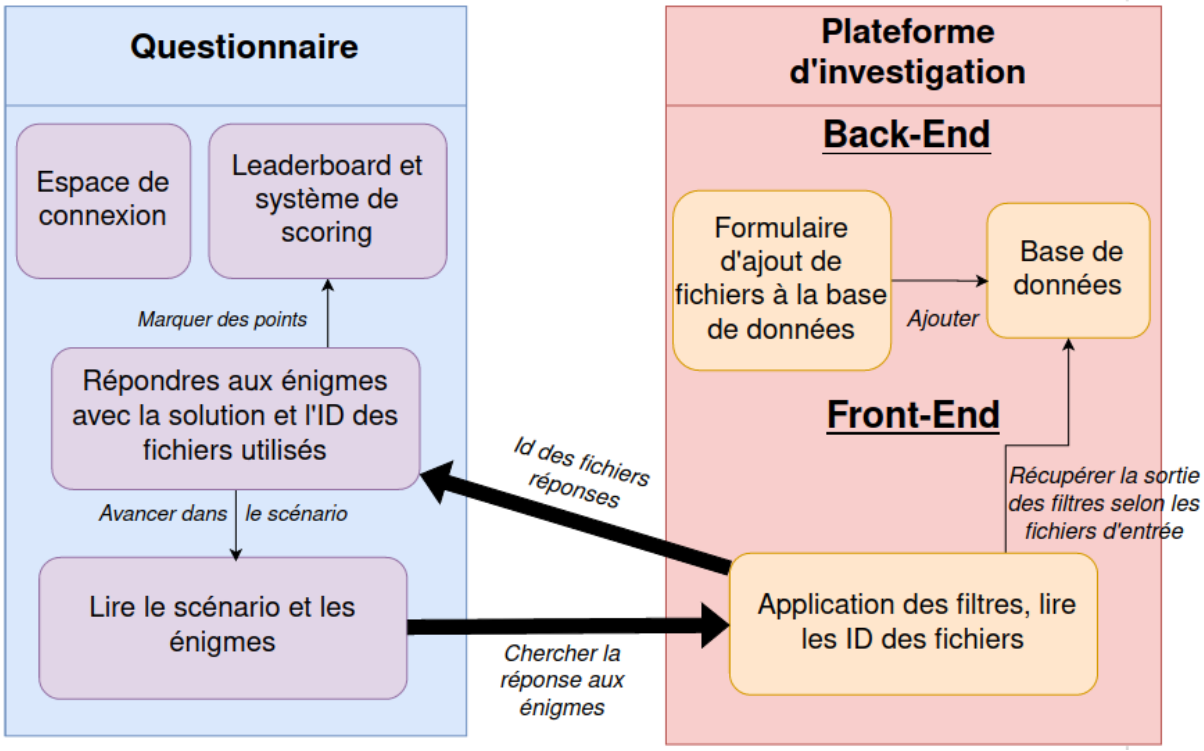

Figure 1: Schéma récapitulalif du projet

3.2. Scénario et Design des énigmes

Nous avons complété en premier le scénario, comme prévu initialement. Il s'agit d'une clé de voûte du projet puisque toutes les énigmes découlent de ce travail.

Chacune d'entre elle a été conçu avec plusieurs objectifs en tête:

- La difficulté, qui nécessite une attention particulière pour que le joueur ne se sente pas dépassé subitement par des pics de difficulté ou au contraire des énigmes qui ne lui donne aucun challenge.

- L’aspect pédagogique, il faut en effet que les mécaniques soient introduites au bon moment pour que le joueur prenne rapidement certains réflexes qui lui seront nécessaires plus tard.

- Développer le scénario et éventuellement ajouter un petit aspect humoristique qui permet de ponctuer le jeu de petites surprises. Ces dernières passent souvent par des “easter eggs” cachés dans certains fichiers ou des éléments de scénario loufoques.

Leur pluralité d’utilité en fait des objets difficiles à créer en maintenant constamment chacun de ces éléments tout au long du jeu. En plus des contraintes d’implémentation de filtre qui peuvent être très restrictives.

Les “fichiers-réponses” des énigmes sont les fichiers fournissant les informations utiles au joueur. Ils peuvent être de nature très différentes (Facture vétérinaire, Biographie Tinder, Spectre audio, QR Code, Image avec watermark, etc ...).

Leur création est essentielle et la quasi-totalité d’entre eux doivent être fait à la main. Certains d’entre eux sont tellement spécifiques qu’ils nécessitent la création de fichier bruit à eux seuls (QR Code, spectre audio, etc ...).

3.3. Front-end du jeu et chiffrement des réponses

Pour les différentes pages du jeu, nous avons opté de faire une page de questions pour un chapitre. Cela permet au joueur de ne pas se noyer dans les questions et au scénario de pouvoir progresser sans pour autant le spoiler. De plus, puisque le travail de vérification des réponses a été fait intégralement en javascript, nous avons chiffré les réponses dans le code pour éviter un maximum la triche de la part des joueurs.

Figure 2 : Interface du jeu

3.4. Plateforme d'investigation

La page internet d'application des filtres est en fait un logiciel qui prend des informations d'une base de données, et crée des éléments html correspondants avec pour but final de créer une page ou le joueur manipule des fichiers d'entrée et où il leur applique des filtres pour résoudre les énigmes. Une plateforme d'investigation en somme.

Ce logiciel est donc unique mais son contenu change à chaque chapitre de l'histoire du jeu, car chaque chapitre contient une database différente.

A gauche de la page, se trouve des fichiers d'un disque dur ou d'une clé-usb fictive, suivant le propos du scénario.

Le joueur peut alors selectionner ces fichiers, et leur appliquer un des filtres du milieu de la page, et appuyer sur le bouton « Filtrer » pour obtenir un résultat si le filtre est applicable.

Nous avons voulu, au travers de cette page, créer notre propre version du logiciel CyberChef, pour permettre au joueur d'en apprendre plus sur la forensique en manipulant lui-même les fichiers.

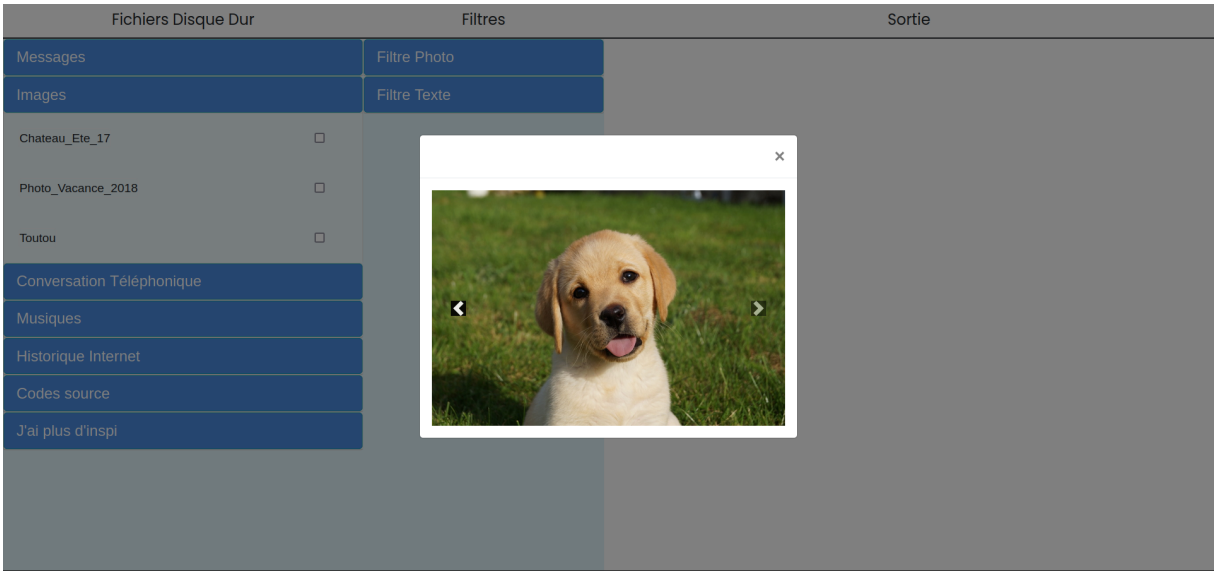

Figure 2: Prévisualisation des fichiers d'entrée

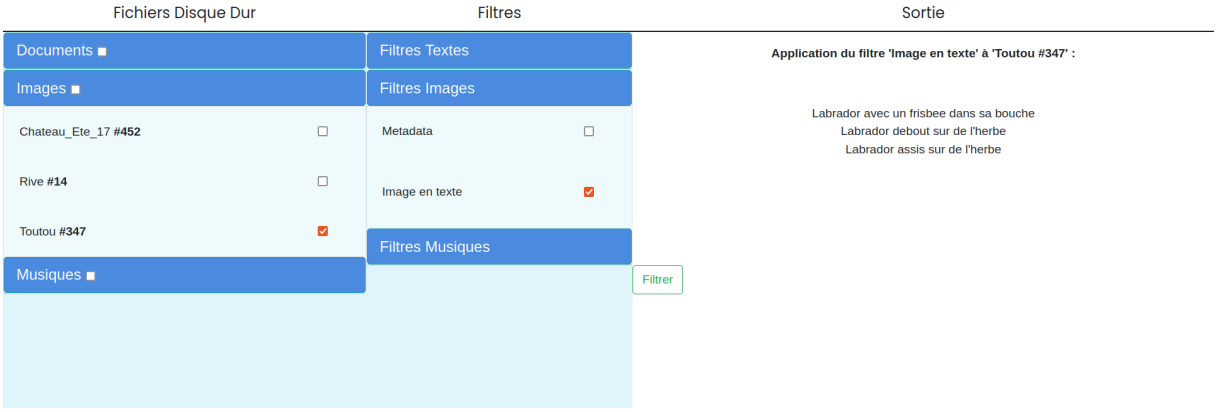

Figure 3: Exemple d'application d'un filtre à un fichier

Les données sont pour l'instant stockées dans une base de donnée au format Json. Chaque chapitre du scénario possède une base de donnée différente, qui repertorie les filtres et leurs sorties pour chaque fichier d'entrée.

```
"Recherche de contenu : Date":[
  {
    "inputName":"monCV",
    "content":"date de naissance: 13 juillet 1982"
  }
],

"Recherche de contenu : Nom Propre":[

  {
    "inputName":"monCV",
    "content":"Jean Forensique | rue de la Forensique"
  },
  {
    "inputName":"CompteRendu",
    "content":"Jean Forensique"
  },
  {
    "inputName":"Adoption",
    "content":"Les Fidèles  Moustachus | 84 Rue Saint Jean | Jean | Forensique | Daug | Labrador | Caen"
  },
  {
    "inputName":"Facture_veto",
    "content":"SIFORENQ Christophe | 35 rue des Tonneliers | Lés Animos | France | Robert Jones | Tensoplast | Labrador "
  }
],
```


Figure 4: Base de données du tutoriel

De plus, il est facile d'ajouter des nouveaux fichiers (« bruit » par exemple ou « leurre ») grâce au formulaire d'ajout que nous avons créé :

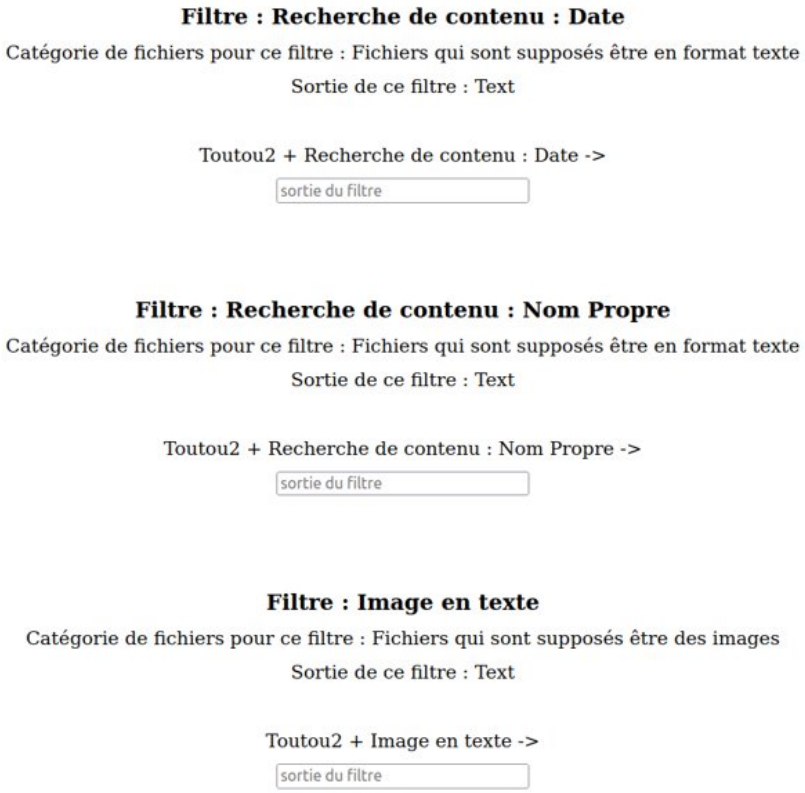

Figure 5: Page d'ajout de fichiers, avec les champs des sorties de filtre à compléter

4. Retours sur le projet

Nous avons effectué une première période de test du jeu avec 5 personnes qui ont joué uniquement sur les 2 premiers chapitres, puis une deuxième session avec 5 autres qui ont pu tester le jeu complet.

Nous avons tenté de diversifier les profils mais finalement nous avons eu 9 élèves de l'ENSICAEN pour 1 seul testeur qui n'était pas lié à l'ENSICAEN.

Le manque de temps ne nous a pas permis d'avoir un résultat de retour sur expérience représentatif mais ces tests ont quand même permis de souligner les points faibles qui nous ont échappé et de valider le travail accompli, car les retours des joueurs-testeurs furent globalement très positifs.

Le point le plus important selon nous était de proposer une expérience ludique et agréable à nos joueurs, et d'après les premiers résultats, cet objectif a globalement été atteint.

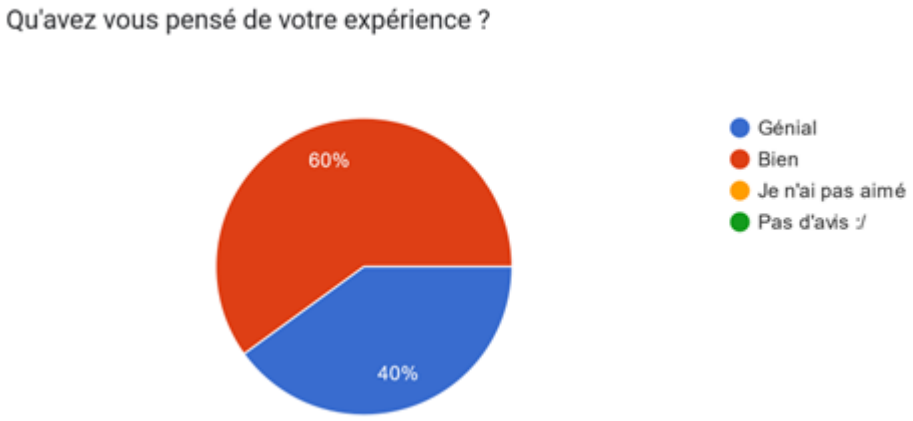

Figure 6: Réponse des 10 testeurs sur la qualité de leur expérience

Malgré tout, une de nos question n'a pas été au goût des bêta-testeurs. Le fichier réponse (un billet d'avion) donnait lieu à des incompréhensions. Nous avons donc modifié cette question après leurs retours.

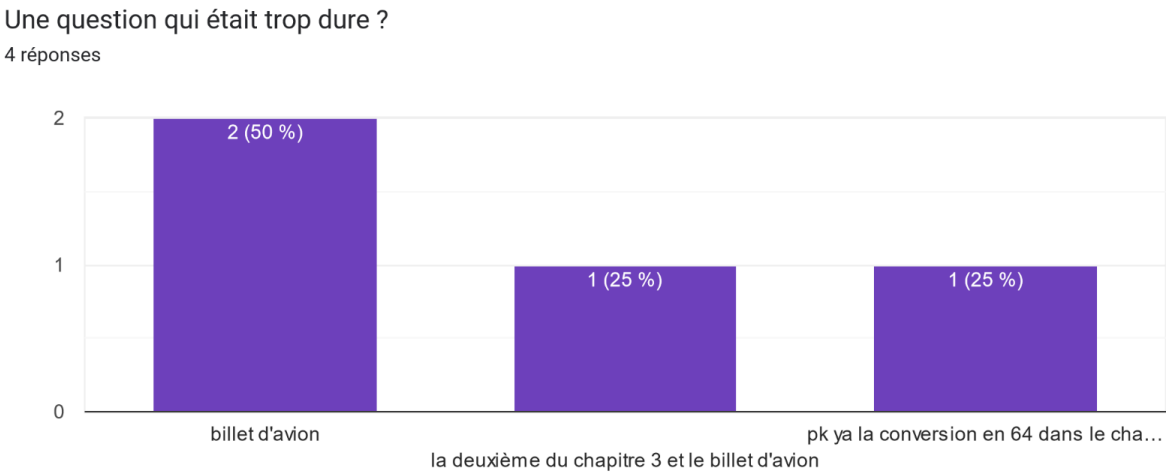

Figure 7: Réponse des 4 testeurs qui ont jugé qu'une question avait été trop compliquée

Quelques utilisateurs nous ont également reporté la faiblesse du chapitre 3 qui aurait dû être le point d'orgue de leur expérience vidéoludique, il faudra donc en tenir compte dans la suite du projet et y apporter des modifications.

chapitre 3 trop flou/ pas compris

couleur du bouton filtre en vert ???

Le chapitre 3 manque de contexte, il faudrait quelque chose de plus immersif. Aussi le passage entre les chapitres est pas très marquant, niveau histoire je pense.

design de la page des filtres très réussi, j'adore la couleur du bouton filtre

Figure 8: Remarques générales sur le jeu (question optionnelle)

5. Méthodologie de travail

Nous avons tout d’abord commencé par travailler avec une méthode classique, dans laquelle nous travaillions régulièrement avec notre groupe sur nos tâches respectives.

Néanmoins, au cours du projet nous avons commencé à effectuer des périodes de sprint plutôt que de travailler chacun de son côté. Cette méthode de travail nous a permis d’arriver beaucoup plus vite à des résultats concrets. Il était aussi beaucoup plus facile de s’adapter en fonction du travail des autres et des modifications sur les objectifs nécessaires à la suite du projet.

Nous avons alors organisé des sprints, des sessions intenses durant lesquelles toute l’équipe travaillait sur des tâches spécifiques. Nous faisions également un bilan après le sprint pour savoir ce qui avait été réalisé, et ce qu’il restait à faire, ainsi que des réunions avant les sprints afin de préciser le contenu du sprint et la répartition des tâches pour chacun.

Nous avons apprécié cette manière de faire, qui permet à toute l’équipe de se coordonner efficacement durant des sessions.

Si le projet était à refaire, nous utiliserions une méthode agile pour tout le projet, car notre groupe n’a pas réussi à bien implémenter la méthode de répartition des travaux traditionnelle.

BILAN

6. Présentation des objectifs atteints

Nous avons atteint la plupart des objectifs que nous nous étions fixés au départ avec monsieur Rosenberger. Si nous détaillons le résultat de ntore projet :

- le scénario du projet, véritable clé de voûte, a été réalisé dès que possible.

- 20 énigmes ont été réalisées avec leurs fichiers d'entrée et de réponses, toutes ont été pensées avec une courbe de difficulté croissante à l'esprit. Facile pour le tutoriel, simple pour le chapitre 1, moyen pour le chapitre 2 et difficile pour le chapitre 3. De plus, il est possible de choisir trois difficultés, collège, lycée ou supérieur ce qui permet de rendre disponible ou non les questions les plus difficiles de chaque chapitre. Quelques fichiers « bruit » ont aussi été créé.

- Un site web a été pensé pour répondre aux différentes questions. Pour valider sa réponse à une énigme, il faut fournir la réponse en elle-même et l'id du fichier qui a permis de répondre pour s'assurer d'éviter la triche. De plus les réponses sont chiffrés.Une fois toutes les énigmes d'un chapitre résolut, il est possible de passer au suivant et de s'attaquer aux énigmes plus ardus. Pour nous aider dans la résolution,

- Un site de filtre a de disque dur a été réalisé pour simuler un outil de recherche forensique. Il est possible de passer chaque fichier au crible pour obtenir un maximum d'informations possible.

- Le front-end de fonctionnalités futures a aussi été réalisé, avec un menu qui contient des liens vers une page de classement, une page de connexion, une page des contributeurs du projet et un retour vers le jeu.

Enfin, nous avons créé des outils pour faciliter le travail des futures équipes qui prendront ce projet, Par exemple, nous avons développé une page html permettant d'ajouter facilement des fichiers bruit dans n'importe quel chapitre du scénario (car chaque scénario utilise des databases différentes).

Ainsi n'importe qui peut rajouter des fichiers bruits et améliorer le jeu, même en n'ayant aucune connaissance informatique.

Nous avons également pensé (avec l'aide de Mr Rosenberger) à l'idée de créer des animations explee pour narrer d'une meilleure manière le scénario et améliorer l'imersion du joueur.

7. Présentation des objectifs non atteints, des motifs et des conséquences.

La constitution des fichiers de la base de données est une tâche chronophage et rébarbative, surtout en ce qui concerne les fichiers dit de “bruit” qui servent à noyer les informations utiles des énigmes dans une masse d’information inutile. L’objectif de ce procédé est de forcer les joueurs à utiliser les filtres pour répondre à leurs questions. Leurs types sont variés et parfois particulièrement longs à mettre en place, comme les photoshop de papiers administratifs par exemple.

En conséquence, il était impossible de concevoir autant de fichiers, même composés de contenu aléatoire.

Mr. Rosenberger nous a donc proposé de s’occuper de cette partie, notamment à l’aide de bases de données du GREYC.

Le chapitre 4 devait être composé d’une seule et unique énigme de grande difficulté, mais avec l’avancement du deadline et le travail nécessaire à sa réalisation nous avons décidé avec notre encadrant de ne pas la créer.

Le back-end du site n’a pas été fait également, ne sachant pas comment nos pages seraient intégrées au site de G’DIP et également par manque de temps.

8. Bilan au sein du groupe

Globalement, notre projet s'est plutôt bien déroulé. Presque tous les membres du groupe se sont vraiment beaucoup investis dans le projet. Nous avons appris que le travail de groupe nécessite une certaine discipline que nous n’avions pas en début d’année et que nous avons réussi à cultiver au fur et à mesure. Ce projet nous a aussi permis de nous rendre compte de l’avantage de la méthode agile pour les projets de développement informatique.

Nous avions opté pour ne pas travailler avec git au début du projet car nos parties de développement étaient très séparées les unes des autres et ce fut une erreur de compréhension de l’utilisation de git. En effet, nous voyons l'outil

comme un moyen de partage de code en oubliant l'aspect de gestion de version. En cours d'année, nous avons appris à mieux nous en servir et nous nous sommes rendu compte qu'il était presque indispensable d'avoir accès à cet outil dans les projets informatiques.

Les contacts avec nos encadrants ont également été positifs, avec beaucoup de questions qui nous troublaient, qui ont finalement été éclairées par leurs conseils.

9. Perspectives du projet

Durant notre projet, et après plusieurs consultations avec notre encadrant Mr Rosenberger, nous avons longuement pensé au devenir du projet, et avons fait en sorte que même si nous ne pouvions pas atteindre tous les objectifs, notre projet soit facile à prendre en main et facilement modifiable par toute équipe ou ingénieur souhaitant l'améliorer.

Ainsi, il est envisageable que d'autres équipes développent les idées et les outils dont nous avons créé une ébauche et que nous avons détaillé dans la partie du bilan du travail réalisé.

Plus généralement, notre projet est stocké sur gitlab, et nous avons essayé de détailler avec des commentaires et des fichiers README tout le travail que nous avons réalisé pour rendre facile l'amélioration ou la modification de notre travail par toute autre équipe informatique.

Notre objectif final, que nous partageons avec notre encadrant Mr Rosenberger, est que ce jeu sur la forensique puisse être déployé en cette fin d'année 2023, ou bien en 2024. Sur le site de G'DIP tout d'abord, mais aussi dans les écoles de Normandie ou de France afin de promouvoir la forensique de manière ludique et, éventuellement, d'organiser des compétitions avec le système de leaderboard.

ENSI CAEN

ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Ecole Publique d'Ingénieurs en 3 ans

6 boulevard Maréchal Juin, CS 45053
14050 CAEN cedex 04

ministère éducation nationale enseignement supérieur recherche
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Normandie Université

Cti Commission des titres d'ingénieur

cdefi Conférence des Directeurs des Écoles Françaises d'Ingénieurs

European Accreditation of Engineering Programmes EUR-ACE®

CONFÉRENCE DES GRANDES ÉCOLES