Ecole Publique d'ingénieures et d'ingénieurs en 3 ans

Rapport

PROJET 2A :
JEU SÉRIEUX SUR L'INVESTIGATION NUMÉRIQUE

Année Universitaire 2024/2025

ANWAR BEG Jawad
FREVILLE Noé
BUI Théo
DOUCOURÉ Araby

Tuteurs : **GIGUET Emmanuel**
GERNOT Tanguy

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

www.ensicaen.fr

TABLE DES MATIERES

1. PRESENTATION 3

1.1. Présentation du projet 3

1.2. Objectifs 3

2. METHODOLOGIE DE TRAVAIL 3

3. SCENARIO ET GAMEPLAY 4

4. ÉVOLUTIONS ET PERSPECTIVES DU PROJET 11

5. BILAN 11

1. Présentation

1.1. Présentation du projet

"*Little White Hat*" est un jeu sérieux sur navigateur de type point and click et visual novel, plongeant le joueur dans l'univers captivant de l'investigation numérique. Dans ce jeu, vous incarnez un jeune stagiaire sous la supervision d'un professeur spécialisé dans l'investigation numérique, vous découvrez progressivement les fondamentaux de l'investigation numérique à travers des exercices et des mises en situation.

Mais tout bascule lorsqu'un événement mystérieux et troublant survient, bouleversant le cadre d'apprentissage initial. Vous vous retrouvez alors plongé au cœur d'une affaire complexe, où vos compétences nouvellement acquises seront mises à rude épreuve.

Au fil du jeu, vous devrez analyser des indices, manipuler des outils spécialisés, et résoudre des énigmes variées basées sur des thématiques clés de l'investigation numérique : stéganographie, analyse de métadonnées, cryptographie et plus encore.

"*Little White Hat*" propose ainsi une expérience ludique et pédagogique, où la logique, l'observation et la méthodologie sont les clés pour progresser et découvrir la vérité.

1.2. Objectifs

L'objectif principal du projet est de concevoir un jeu sérieux sur l'investigation numérique, accessible aux élèves de collège et lycée. À travers une approche ludique et interactive, ce jeu vise à leur faire découvrir les principes fondamentaux de la cybersécurité et de l'investigation numérique.

Au-delà de son aspect éducatif, ce projet représente également un défi technique pour nous. Il nous permet d'approfondir nos compétences en développement web tout en découvrant des techniques d'investigation numérique et en essayant de proposer une expérience de jeu fluide, immersive et accessible directement depuis un navigateur.

2. Méthodologie de travail

Au début du projet, toute l'équipe a collaboré autour d'un brainstorming sur l'ensemble des aspects du jeu, permettant une réflexion commune sur le concept, les mécaniques et la direction générale du projet. Une fois les bases établies, nous avons réparti les tâches en fonction des compétences et des intérêts de chacun :

La première étape a été de rédiger un scénario capable d'intéresser les joueurs donc nous sommes partis sur une intrigue qui mélange énigme, quête et sauvetage. C'est Araby qui s'est

chargé de l'écriture du scénario donc la création du fil conducteur narratif, le développement des personnages, leurs dialogues et la mise en place des intrigues qui rythment l'expérience de jeu.

Jawad et Théo ont participés à la conception des différentes énigmes du jeu avec Araby pour garder une cohérence de l'univers et sont ensuite passer à leur développement, en s'assurant qu'elles soient à la fois stimulantes et pédagogiques.

Noé a travaillé sur le développement et la mise en place de l'interface utilisateur, en veillant à une expérience fluide et intuitive, ainsi qu'à l'intégration des énigmes dans le gameplay.

Et une fois toutes les étapes de conceptions terminer, nous nous sommes réparti les chapitres pour avancer au maximum sur leurs développements.

Nous étions principalement en présentiel lors des séances de travail ce qui permettaient des échanges plus libres et spontanés, de travailler en équipe que ce soit tous ensemble ou par binôme. Être tous ensemble permettaient aussi de stimuler la créativité et forcer la remise en question puisque l'on doit partager ses idées, donner son avis, débattre sur l'utilité, l'intérêt de celles-ci. Et pour le travail complémentaire nous restions quand même en contact soit par message, soit par appel.

Nos tuteurs organisaient plusieurs réunions, à peu près hebdomadaires, pour être tenu au courant de nos avancées et nous guider si jamais quelque chose n'allait pas.

Cette organisation nous a permis de travailler efficacement tout en conservant une vision commune et cohérente du projet.

3. Scénario et gameplay

Nous avons décidé de séparer l'histoire en 5 chapitres, apportant chacun une touche d'histoire et des défis.

Prologue (Chapitre 0) :

Vous êtes en stage chez un professeur en cybersécurité/forensique. Grand amateur d'énigmes et de puzzles, il vous propose, à la fin de la journée, un défi basé sur la stéganographie. Caché dans une image, un QR code mène à un mot de passe chiffré par le chiffrement de César – donnant accès à son ordinateur. Avant de partir, il vous demande de venir un peu plus tard que d'habitude le lendemain.

Pour réaliser cette énigme nous avons utilisé la méthode des bits de poids faible. Nous avons deux images : l'une correspond au QR code et l'autre à une image représentant la statue de Jules César. Nous avons remplacé les bits de poids faible de l'image de césar par ceux du QR code. Ainsi, le QR code est contenu dans l'image de césar sans être visible.

Chapitre 1 :

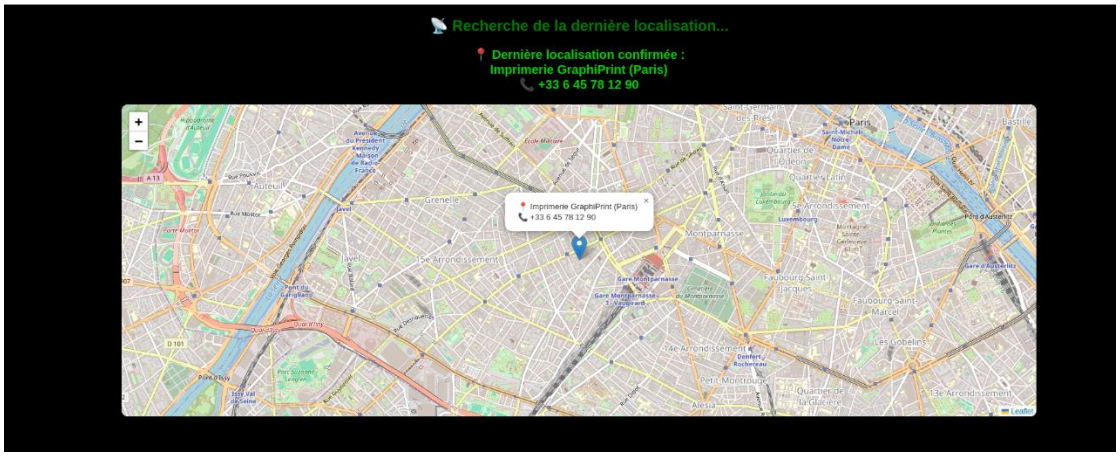
Le lendemain, le professeur se fait attendre et ne semble pas répondre au téléphone. Sans lui, vous ne pouvez pas entrer dans le laboratoire. Vous décidez donc d'aller prendre de ses nouvelles directement chez lui.

Arrivé chez lui, la porte est entrouverte et vous tombez nez à nez avec un inconnu. Celui-ci vous explique qu'il est inspecteur de police et avait normalement rendez-vous avec le professeur, mais qu'il a trouvé son appartement dans un état inquiétant. Vous tentez d'appeler le professeur une dernière fois et entendez la sonnerie résonner à l'intérieur. Son téléphone est toujours là. Mauvais signe.

L'inspecteur est formel : le professeur est en danger. Vous devez le retrouver au plus vite. En fouillant son téléphone, vous tombez sur une piste qui mène à une imprimerie, située en zone industrielle.

La piste en question est une notification de la dernière personne qui l'a contacté. L'apprenti utilise un outil de traçage de téléphone lui permettant d'obtenir la dernière localisation connue de la personne. Il saisit son numéro de téléphone dans l'outil, qui lui indique sa dernière position avant que l'appareil soit éteint. C'est ainsi qu'il découvre que cette localisation correspond à une imprimerie.

Pour ce faire, nous avons créé une interface "Traçage de téléphone" dans laquelle l'utilisateur saisit le numéro de téléphone. Le scan dure cinq secondes, après quoi les coordonnées GPS associées au numéro apparaissent. Une carte interactive s'affiche ensuite, indiquant l'emplacement.

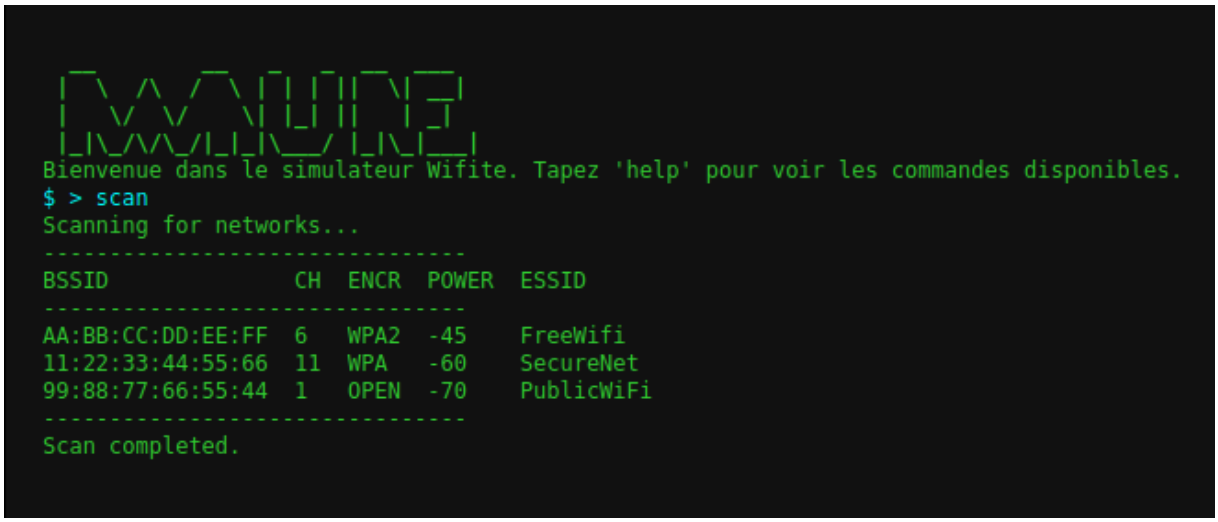


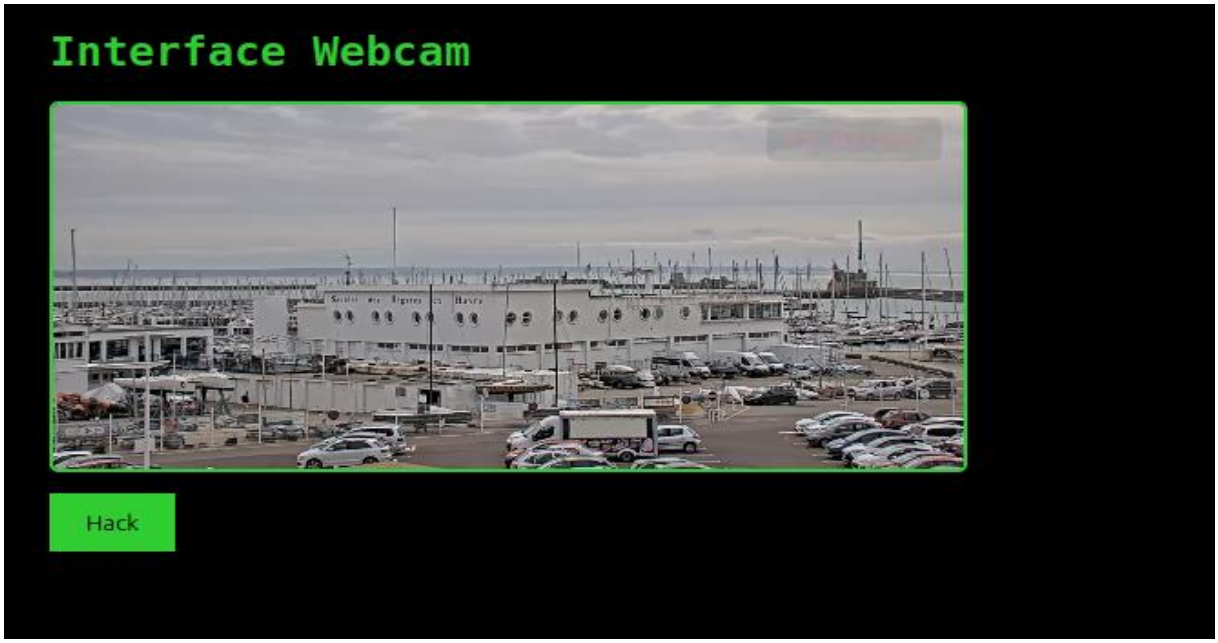
Chapitre 2 :

La zone est gardée, mais vous décidez tout de même de vous y infiltrer. Dans la salle des moniteurs, vous prenez le contrôle des flux vidéo pour couvrir l'avancée de l'inspecteur. Mission accomplie : il revient sain et sauf, et vous fait part de sa découverte : cette imprimerie fabrique de faux documents.

Vous proposez d'alerter la police, mais l'inspecteur vous arrête. Il vous confie alors un secret : il n'est plus en service. Autrefois inspecteur, il a été démis de ses fonctions après un incident impliquant la mafia. Pourtant, il n'a jamais cessé de traquer l'organisation et cherche à se venger. Le professeur était son allié dans cette quête, et leur rendez-vous manqué devait lui révéler des découvertes cruciales.

Pour éviter de se faire repérer, l'apprenti pirate une caméra de l'imprimerie. Il branche un adaptateur Wi-Fi à son ordinateur et lance wifite sur son terminal pour détecter le réseau Wi-Fi, puis l'attaquer. Nous avons simulé l'interface de wifite pour renforcer l'immersion. Wifite attaque le réseau et donne le mot de passe. Après cela l'apprenti est redirigé vers la webcam avec un bouton "Hack" qui lui permet d'afficher "Un problème est survenu. Veuillez patienter 10 secondes...". Cela permettra l'inspecteur d'entrée dans l'imprimerie.

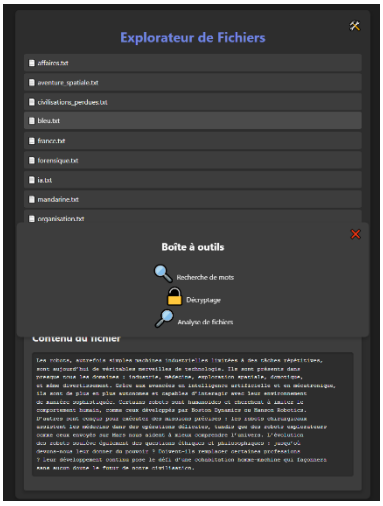




Chapitre 3 :

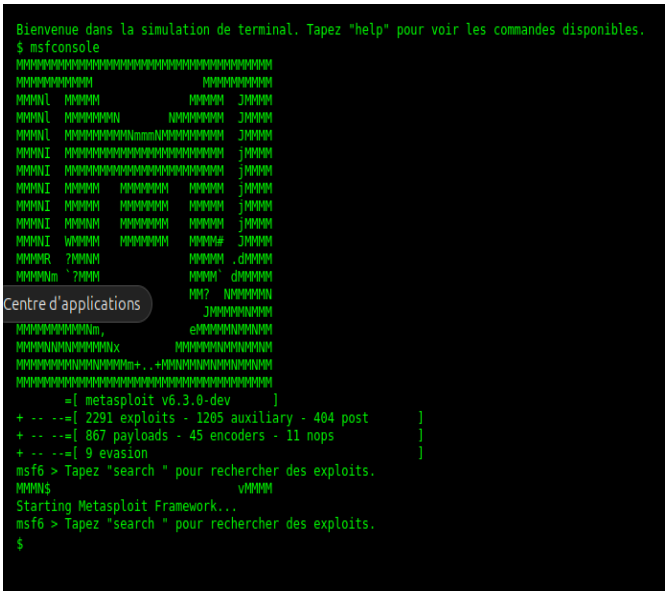
Grâce à la carte d'accès du professeur récupérée chez lui, vous entrez enfin dans son laboratoire. Le mot de passe étant inchangé depuis la veille, vous accédez à son ordinateur. En fouillant ses fichiers, vous découvrez qu'il tentait d'infiltrer un serveur. Il semblait enfin avoir réussi à déchiffrer les messages d'un forum. Vous apprenez que ce chiffrement par cryptographie distribuée possède trois auteurs, dont l'un d'eux est le professeur.

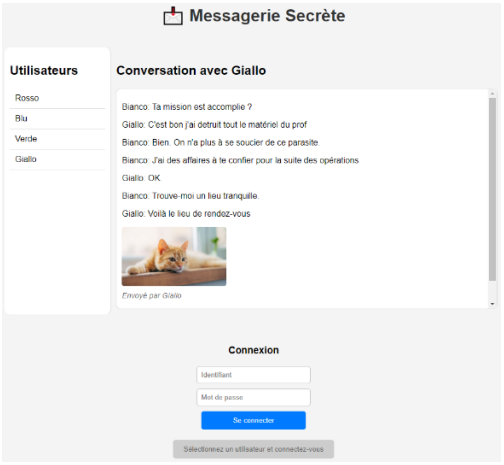
Vous retrouvez un échange avec la personne qui a saccagé son appartement et décidez de lui tendre un piège.



Au début, on trouve une série de fichiers textes portant sur des sujets, mais sans plus. En utilisant une simulation d'outil d'analyse de fichiers, on découvre un indice concernant un potentiel fichier crypté portant une signature cryptographique. Ensuite, il faut trouver la clé pour pouvoir procéder au décryptage. Pour cela, on utilise un outil de recherche de mots qui permet de chercher un indice, et l'un des mots-clés pour trouver la clé est le titre du fichier crypté, lequel apparaît dans un seul autre fichier texte que celui crypté. Une fois la clé découverte, on obtient le fichier en clair grâce à un troisième outil, qui demande le nom du fichier et sa clé pour le décoder. Ce fichier révèle une adresse IP menant au serveur de la Mafia.

Après avoir trouvé un fichier contenant l'IP du serveur de la mafia, l'apprenti tente de le lancer sur le web. Une page s'affiche alors avec le message "Serveur indisponible". Il décide alors de rechercher s'il n'y a pas d'informations cachées sur ce serveur. L'apprenti doit effectuer un scan du serveur avec nmap pour identifier les ports ouverts et les versions des services, afin de repérer d'éventuelles failles associées. Une fois les failles découvertes, il utilise Metasploit pour exploiter ces vulnérabilités. Les outils Metasploit et nmap ne sont pas les versions réelles, mais sont simulés dans le jeu pour l'immersion.





Dans le serveur de la Mafia, on découvre une faille menant vers le serveur secondaire de l'administrateur de la Mafia. On ne trouve aucune information sur l'administrateur, hormis sa messagerie privée avec d'autres membres de la Mafia, les logs du serveur, et un étrange outil permettant de lire et écrire des métadonnées. En lisant la messagerie, on s'aperçoit qu'un certain membre de la Mafia, portant le nom de code Giallo, est à l'origine du saccage chez le professeur. On découvre que Giallo a fixé un rendez-vous avec l'administrateur, mais qu'aucune information de lieu n'est indiquée : il y a seulement une photo de chat. En analysant les métadonnées, on remarque qu'il y a des coordonnées GPS dans l'image du chat, et qu'une partie des informations échangées entre les différents membres de la Mafia est dissimulée dans les métadonnées des images. On sait que pour piéger Giallo, il va falloir lui donner une image avec un lieu, de préférence qui a un lien avec la mafia, mais qui n'est pas occupé.

L'identifiant "Bianco" est découvert dans les messages : c'est le nom de l'administrateur. Le mot de passe "Poppy" est trouvé dans les métadonnées d'une photo de chien envoyé par Bianco. Quant aux logs, ils révèlent que l'entrepôt de la mafia est abandonné la plupart du temps car les cargaisons stockées là-bas ne reste jamais longtemps. L'adresse MAC de l'entrepôt est trouvée dans les logs, permettant d'obtenir les coordonnées GPS. Ces coordonnées sont ajoutées à 'cheval.jpg' via un outil simulé de métadonnées. L'image est ensuite envoyée à Giallo via la messagerie, avec vérification des coordonnées avant l'envoi accompagné d'un message d'urgence. Giallo croit que l'administrateur Bianco a vraiment un problème et tombe dans le piège. La plupart des outils d'analyse et d'écriture de métadonnées, ainsi que l'outil pour analyser les adresses MAC de routeurs Wi-Fi, sont simulés. En effet, toutes les informations de géolocalisation et les adresses MAC sont factices, l'objectif étant de souligner le principe et les méthodes d'investigation plutôt qu'être fidèle à la technique.

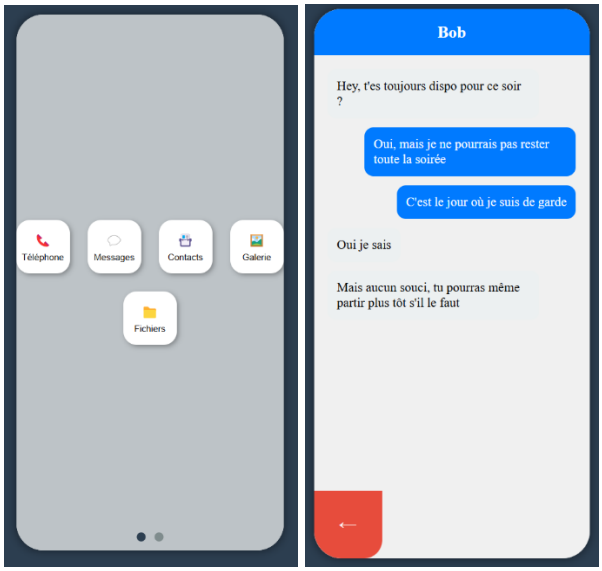
Chapitre 4 :

Une fois le suspect appréhendé par l'inspecteur, celui-ci vous confie son téléphone, déverrouillé par biométrie, pour que vous trouviez de nouvelles pistes. Pendant que l'inspecteur interroge le membre de la mafia, qui refuse de coopérer, vous l'aidez à repérer les incohérences dans ses déclarations.

Le suspect finit par admettre être passé chez le professeur, mais affirme que celui-ci n'était déjà plus là. Il confirme que le professeur était autrefois un haut gradé de la mafia et qu'il a sûrement fui dans un autre pays. L'inspecteur, déçu mais résigné, relâche le mafieux qui s'empresse de disparaître. Quant à vous, votre aventure s'arrête ici, vous êtes trop jeune pour aller plus loin dans cette aventure.

Cette partie se divise en deux phase :

La première est une enquête où l'on fouille le téléphone de l'assaillant à la recherche de preuves et d'indices. Pour cela nous avons simulé l'écran d'un smartphone contenant plusieurs applications comme les contacts, la messagerie, la galerie, l'agenda, …



Dans la seconde, nous confrontons et interrogeons cet assaillant. Ses témoignages et alibis posséderont des incohérences que l'on peut démontrer à l'aide des éléments récupérés précédemment. C'est un style de gameplay originaire de la série de jeu "Ace Attorney" où l'on peut soit attaquer les dépositions des personnages pour obtenir plus de renseignement ou présenter une preuve qui le contredit pour le coincer.

Chapitre 5

Quelques jours plus tard, vous recevez un message du professeur. Celui-ci vous envoie "son dernier casse-tête".

L'idée de ce chapitre était de pouvoir retrouver le professeur grâce aux compétences apprise jusqu'ici (fouille de fichier, analyse de métadonnées, décryptage...). C'est un chapitre bonus dans lequel aucun indice ne sera donné. Malheureusement nous n'avons pas pu l'implémenter car il fallait penser à de nouvelles énigmes un peu plus difficiles et éviter l'effet doublon.

4. Évolutions et perspectives du projet

À l'avenir, plusieurs pistes d'amélioration et d'extension du projet pourraient être envisagées pour enrichir l'expérience de jeu et toucher un public plus large.

- Hébergement : Actuellement il faut le code source du jeu pour pouvoir y jouer ce qui n'est pas des plus pratique donc il faudrait pouvoir l'héberger sur un serveur
- Amélioration des graphismes : Le jeu n'est pas satisfaisant visuellement dû au manque de graphiste/designer dans l'équipe, nous avions essayé d'utiliser un moteur de jeu (Unreal Engine) pour faire les pièces mais la prise en main n'était pas aisée. Donc nous sommes plutôt partis sur des images statiques trouvées sur internet et d'autres générées par IA. Une direction artistique plus affirmée pourrait être développée, avec des visuels plus détaillés et une identité graphique unique.
- Expérience plus interactive : L'ajout d'une bande sonore, l'intégration d'éléments plus dynamiques, comme des animations ou des mini-jeux interactifs, pourraient rendre l'expérience encore plus immersive.
- Difficulté variable : Le jeu n'est pas si simple, pour un novice il peu s'avérer un peu rebutant or le public cible devrait être des collégien et lycéen. Proposer d'autre mode de difficulté que ce soit un plus simple ou un plus difficile pourrait augmenter l'appréciation des joueurs
- Ajout de nouveaux chapitres : L'histoire pourrait être approfondie en intégrant de nouveaux scénarios et défis, permettant aux joueurs d'explorer des enquêtes plus complexes et d'acquérir des connaissances avancées en investigation numérique et cybersécurité.
- Une suite au jeu : Une seconde aventure pourrait voir le jour, introduisant de nouveaux personnages, de nouvelles mécaniques de jeu et un scénario encore plus immersif.

5. Bilan

Nous avons bien apprécié ce projet et nous remercions nos tuteurs pour nous l'avoir confié. Étant déjà habitués à travailler ensemble, l'organisation s'est déroulée sans réelle difficulté.

La liberté offerte par ce sujet était à la fois attrayante et intimidante, mais étant passionnés de jeux vidéo, nous avons voulu relever le défi.

Il y a plusieurs choses que l'on a dû modifier ou remplacé car la réalisation était trop difficile pour nous. Comme avec le passage de l'infiltration dans l'imprimerie, qui devait mélangeait action, observation et réflexion mais pour cela il nous fallait simuler des enregistrements vidéo avec des personnages en mouvement dans une sorte de labyrinthe et personne ne pouvait le faire.

De même pour le scénario et les énigmes, on a fait le choix de garder une certaine cohérence, une certaine réalité donc ce n'était pas simple de trouver le bon équilibre entre les deux. On peut prendre en exemple le téléphone du professeur que l'on retrouve, pouvoir le déverrouiller avec le hack permettrait plus de possibilité à l'histoire mais étant un chercheur en cybersécurité, on ne pouvait pas lui donner un mot de passe facilement trouvable.

Donc oui c'était difficile, surtout quand l'exécution ne pouvait suivre notre créativité, mais toujours intéressant et enrichissant. Cette expérience nous a une fois de plus démontré à quel point créer un jeux vidéo est complexe et requiert une diversité de compétences.

ENSI CAEN

ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Ecole Publique d'ingénieures et d'ingénieurs en 3 ans

6 boulevard Maréchal Juin, CS 45053

14050 CAEN cedex 04