CHARTE DE PROJET

CONSTAT BOX

Version : 2.0

Date : 28/01/2026

Client : OFAC – Police Nationale
Réalisation : Étudiants I2 – 3iL Ingénieurs

Table des matières

1 CONTEXTE

Dans la région Nouvelle-Aquitaine, et plus particulièrement à Limoges, la prolifération des appareils numériques, réseaux domestiques et objets connectés entraîne une augmentation significative des scènes de crime comportant des preuves numériques.

Les enquêteurs de terrain ne disposent pas toujours des compétences techniques ni des outils adaptés pour effectuer rapidement des constats numériques fiables lors des premières phases d'intervention. Cette situation représente à la fois un problème opérationnel et une opportunité d'innovation.

Le projet **CONSTAT BOX** vise à développer un kit d'investigation numérique de premier niveau, autonome et sécurisé, capable de capturer l'état d'un réseau domestique (Wi-Fi, Bluetooth, Ethernet) au moment précis de la saisie, tout en respectant les exigences strictes de la chaîne de preuve judiciaire.

2 OBJECTIFS DU PROJET

L'objectif principal est de fournir un support opérationnel fiable permettant de produire des éléments exploitables dans le cadre d'une enquête judiciaire. L'outil doit **figer et préserver** les preuves numériques présentes sur une scène (réseaux Wi-Fi, appareils connectés, équipements réseaux).

2.1 Objectifs Spécifiques

- **Autonomie totale :** Système fonctionnant sur batterie, sans dépendance électrique au suspect.
- **Simplicité :** Interface accessible à des utilisateurs non-spécialistes (OPJ).
- **Intégrité :** Mécanismes de hachage (SHA-256) pour garantir l'inaltérabilité des preuves.
- **Discrétion ("Zéro Trace") :** Minimiser l'empreinte sur le réseau analysé.

3 VISION ET ARCHITECTURE TECHNIQUE

Le projet évolue vers une architecture client-serveur locale, assurant une parfaite isolation et l'absence de dépendance au Cloud. Le Raspberry Pi agit comme une "sonde" technique fixe, tandis que le smartphone de l'enquêteur sert d'interface mobile et de capteur d'appoint.

3.1 L'Architecture

1. **Le Cerveau (L'Unité Centrale - Raspberry Pi 5) :**
   - Branché en RJ45 à la box Internet du suspect.
   - Exécute les scans lourds (IP, ARP, Wireshark, interrogation API Box).
   - Héberge le serveur Web local et la base de données.
2. **L'Interface (Smartphone / Tablette) :**
   - Connectée au Wi-Fi de la box ou au point d'accès sécurisé du Pi.

   — Permet à l'enquêteur de piloter la perquisition via une Web App responsive.

3. **Le Capteur Mobile :**
   — Le téléphone utilise ses propres capteurs pour scanner le Bluetooth environnant (objets connectés, montres, trackers).
   — Prend des photos des dispositifs découverts pour les joindre au rapport.

3.2 Spécifications Matérielles

Pour répondre aux exigences de rapidité et de "Zéro Trace", le matériel suivant est requis :

— **Calcul :** Raspberry Pi 5 (8 Go RAM) pour gérer les scans lourds et le chiffrement rapide.
— **Refroidissement :** Boîtier avec refroidissement actif indispensable.
— **Connexion :** Câble Ethernet Blindé (RJ45 Cat 6a) et Adaptateur Wi-Fi haute puissance (Monitor Mode).
— **Stockage :** Carte MicroSD Haute Vitesse (V30) pour l'OS (Kali Linux) et Clé USB 64 Go pour l'export "propre" des preuves.
— **Énergie :** Batterie externe (Power Bank) 20 000 mAh (Sortie 25W) pour une autonomie totale, avec câble USB-C à interrupteur physique.

4 FONCTIONNEMENT PAR PHASE

4.1 Phase I : Identification & Scan Réseau (Automatisé par le Pi)

— **Scan Passif & Actif :** Analyse ARP pour lister les machines, y compris celles bloquant le "ping".
— **Détection de "Fantômes" :** Identification d'IP sans adresse MAC physique évidente (VM, serveurs cachés).
— **Analyse de Trafic :** Capture Wireshark pour identifier les comportements (ex : flux flux vidéo = caméra IP).
— **API FAI :** Interrogation directe des Box (Orange, Free, SFR...) pour récupérer baux DHCP et historiques.

4.2 Phase II : Étude de Proximité (Via le Smartphone)

— **Scan Bluetooth :** Détection des objets à proximité immédiate de l'enquêteur.
— **Documentation Photo :** Chaque appareil détecté génère une "fiche technique". L'enquêteur prend une photo via l'app, qui est immédiatement hachée et stockée sur le Pi.

4.3 Phase III : La Checklist de Perquisition

C'est le cœur métier de l'outil. L'application confronte la vision réseau à la réalité physique.

— **Fiches Dynamiques :** Une fiche par IP/MAC détectée.

— **Mode Checklist :** L'OPJ valide ("coche") chaque appareil physiquement saisi.

— **Alertes Exotiques :** Notification immédiate en cas de détection suspecte (VPN, Proxy, MAC Randomization).

5 GÉNÉRATION DU PROCÈS-VERBAL (PV)

L'application automatise la rédaction administrative pour garantir la validité juridique :

— **Horodatage Certifié :** Vérification croisée (Box / Système / Heure réelle) pour éviter toute manipulation.

— **Rédaction Automatique :** Génération d'un texte structuré prémâché (e.g., *"Le [Date] à [Heure], l'analyse a révélé..."*).

— **Assistance IA :** Suggestion d'identification pour les appareils inconnus (signature réseau).

6 PÉRIMÈTRE

Inclus :

— Développement de l'outil d'analyse réseau autonome (Backend Python/Kali).

— Interface Web responsive pour smartphone/tablette.

— Création de l'image système sécurisée (Raspberry Pi).

— Système de génération de rapports chiffrés et horodatés.

— Documentation technique et guide utilisateur.

Exclus (ou optionnel) :

— Analyse des réseaux cellulaires (GSM/4G/5G).

— Analyse forensique approfondie (récupération de données effacées sur les disques durs saisis). Mots de passe Wi-Fi (cracking).

7 LIVRABLES ATTENDUS

1. Une **sonde "ConstatBox"** (Raspberry Pi configuré) prête à l'emploi.
2. Une **Application Web** de pilotage, déployée localement sur la sonde.
3. Un module de génération de rapports PDF/PV.
4. Une documentation technique d'installation et de maintenance.
5. Un manuel utilisateur simplifié pour les enquêteurs.
6. Une démonstration fonctionnelle du prototype final.

8 PARTIES PRENANTES

— **Client / Expert Métier :** OFAC – Police Nationale (Valide les besoins fonctionnels et juridiques).

— **Réalisation :** Étudiants I2 – 3iL Ingénieurs (Conception et développement).

— **Supervision :** Encadrants pédagogiques 3iL.

— **Utilisateurs Finaux :** Enquêteurs de terrain / OPJ.

9 BUDGET ET RESSOURCES

Le projet s'inscrit dans un cadre pédagogique.

— **Budget :** Limité, valorisation du temps de travail de l'équipe.

— **Matériel :** Utilisation de matériel existant ou acquisition à faible coût (Raspberry Pi 5, Accessoires réseau, Power Bank).

— **Logiciel :** Solutions Open Source privilégiées (Kali Linux, Python, Wireshark).

10 RISQUES

— **Juridique :** Non-conformité des rapports aux exigences de procédure pénale. *Mitigation : Validation régulière avec l'OFAC.*

— **Technique :** Instabilité de l'analyse réseau ou surchauffe du matériel. *Mitigation : Choix du Pi 5 avec refroidissement actif et tests intensifs.*

— **Sécuritaire :** Compromission des données saisies. *Mitigation : Chiffrement et hachage systématique.*

— **Calendaire :** Contraintes académiques fortes. *Mitigation : Méthodologie Agile et priorisation des features (MoSCoW).*