



A.P.L Consultants

ZAC des Varannes

9, rue des guettes 45140 Ingré (France)

Tél : + 33 (0) 238 742 220

Fax : + 33 (0) 238 746 327

E mail : ap.laclotte@apl-consultants.com

<http://www.apl-consultants.com>

MANUEL D'INSTRUCTIONS BLOODHOUND



BLOODHOUND

Sommaire

Chapitre	Description	Page
1	Introduction	2
2	Description du système	3
3	Utilisation du système	6
4	Performances du système	8
5	Optimisation de l'environnement de recherche	10
6	Fausses Réponses	11
7	Techniques de recherche	12
8	Technologie	13
9	Traceur de Câble	14
10	Illumination de Câble	14
11	Spécifications	14
12	Entretien régulier et réglages	14

1. Introduction

1.1 Présentation du *Bloodhound* :

Le *BloodHound* est un équipement électronique, à l'usage des équipes effectuant des Opérations de Sécurité Electronique (OSE), permettant la détection de systèmes d'écoute clandestins. Celui-ci fonctionne par détection du champ électrique créé par un microphone en activité, et convertit ce champ électrique soit en un signal audio que l'opérateur peut écouter soit en un bouclage acoustique.

1.2 Le *BloodHound* peut être utilisé pour détecter les types d'attaques suivants :

- a) Microphones filaires alimentés ou amplifiés
- b) Piégeages Téléphoniques (filaires ou radiofréquences)
- c) Microphones utilisant un support Radiofréquence
- e) Microphone utilisant une technologie par Courant Porteur
- f) Enregistreurs
- g) Caméra vidéo de type filaire

Tous ces appareils, intégrant des amplificateurs audio, créent un champ électrique détectable par le *BloodHound*. Dans le cas de la vidéo le champ émis est particulier et facilement identifiable.

1.3 En plus de l'utilisation normale, le *BloodHound* peut être utilisé pour les fonctions suivantes :

- a) Amplification audio d'usage général. En particulier sur les signaux très faibles et /ou ayant un fort niveau de bruit.
- b) Traceur de lignes.

2. Description du système

2.1 Le système *BloodHound* se compose des éléments suivants:

- 1 Sonde
- 1 Unité de filtrage (avec sacoche et ceinture)
- 1 Unité Amplificateur de puissance
- 1 Casque
- 2 Câbles coaxiaux BNC-BNC (d'une longueur de 1 mètre)
- 1 Câble coaxial BNC-BNC (d'une longueur de 2 mètres)
- 1 Câble coaxial BNC-BNC (d'une longueur de 3 mètres)
- 1 Câble coaxial BNC-Pinces croco (d'une longueur de 1 mètre)
- 1 Câble coaxial BNC-Jack 3,5MM (d'une longueur de 1 mètre)
- 1 Enregistreur/radio portable style Walkman
- 1 Casque anti-bruit
- 1 Chargeur de batterie
- 1 Antenne rigide
- 1 Perche télescopique
- 6 Piles AA
- 2 Piles PP3
- 1 Soufflette
- 1 Micro filaire test
- 1 Valise de transport

2.2 Sonde

Elle est constituée d'un petit appareil portable équipé d'une prise pour l'antenne à une extrémité, et d'un connecteur BNC à l'autre extrémité. La sonde, agissant en tant que détecteur de champ électrique du système, contient des amplificateurs à haute impédance d'entrée et le filtrage. La sonde ne nécessite pas de piles, puisqu'elle est alimentée par l'unité de filtrage par via le câble de connexion. La sonde ne possède pas de réglage.

2.3 Filtre

Le filtre est un petit ensemble indépendant équipé d'une ceinture permettant à l'opérateur de le porter autour de la taille.

Le filtre est un processeur de signal sophistiqué qui élimine les interférences du signal détecté par la sonde, en fournissant un signal à l'opérateur par le casque audio et au système amplificateur de puissance par la sortie BNC (output). Le filtre possède les contrôles et les indicateurs suivants :

- a) **Prise d'entrée (Input)** : Une prise B.N.C. qui se connecte à la sonde. Celle-ci reçoit le signal de la sonde, et lui fournit son alimentation.
- b) **Prise de sortie (Output)** : Un connecteur B.N.C permettant la connexion à l'Amplificateur de Puissance (P.A) ou à un équipement d'enregistrement selon le cas. La sortie est à tension constante de 1V c-c.
- c) **Bouton Null** : Il s'agit d'un contrôle rotatif (dix tours) qui est utilisé pour ajuster l'annulation des principales harmoniques dûes au courant alternatif du secteur.
- d) **Interrupteur Null (contrôle interne)** : Celui-ci permet de sélectionner la fréquence de l'alimentation secteur dont il faut annuler les harmoniques : soit 50 Hz ou 60 Hz.
- e) **Bouton Vol** : Ce contrôle rotatif règle le niveau de sortie du casque audio. Il est à noter que le filtre comprend un circuit compresseur très efficace qui ajuste constamment le gain du système afin d'assurer le maximum de sensibilité, quel que soit le système d'entrée.
- f) **Prise casque** : Une prise casque permet la connexion du casque audio de l'opérateur.
- g) **POWER**. Un voyant vert qui s'allume lorsque le filtre est sous tension.
- h) **Indicateur de batteries BAT**. Celui-ci, de couleur ambre, s'allume lorsque les piles du filtre sont presque épuisées.

2.4 Amplificateur de puissance (P.A.)

L'unité P.A. contient un amplificateur audio, un haut-parleur, un générateur de signaux audio, et une alimentation à batterie rechargeable. Il est équipé des contrôles et indicateurs suivants :

- a) **Connecteur d'entrée de chargeur batterie** : Il permet la connexion du chargeur de batterie. Un indicateur rouge confirme la mise en charge.
- b) **Un indicateur de batterie faible (jaune)**.
- c) **Prise entrée (INPUT)** : Une prise B.N.C. pour la connexion à l'unité de filtrage, ou la plupart des appareils audio.
- d) **Prise sortie (OUTPUT)** : Un connecteur B.N.C. de sortie permettant l'utilisation de l'ampli de puissance pour tracer des lignes, et d'autres fonctions secondaires.
- e) **ON/VOL** : Interrupteur rotatif mettant en service le système, et ajustant le volume du son.
- f) **DC ON** : Un voyant vert qui s'allume lorsque le P.A. est sous tension (c'est-à-dire, lorsque l'interrupteur **ON/VOL** de contrôle est positionné sur ON).
- g) **L.S./OUTPUT** : L'amplificateur de puissance de sortie est réglé soit sur **L.S.** (haut-parleur interne) ou dirige le signal vers le connecteur B.N.C. de sortie.
- h) **SWEEP/ON/OFF** : Ce commutateur actionne le générateur de tonalités interne.
- i) **Contrôle SWEEP** : Un contrôle rotatif qui ajuste la vitesse de balayage du générateur de tonalités interne.

3. Utilisation du système

3.1 Présentation

Le *BloodHound* est l'un des outils mis à la disposition de l'opérateur d'OSE. Son utilisation devrait être planifiée de concert avec le reste des équipements afin de maximiser les chances de celui-ci de découvrir des attaques techniques tout en minimisant le risque d'alerter le poste d'écoute adverse qui pourrait l'amener à mettre en place des contre-mesures efficaces.

Le système *BloodHound* peut être utilisé afin de détecter un microphone espion grâce à deux mode : **Passif ou Actif**. Une opération typique pourrait utiliser soit le mode passif, le mode actif ou bien les deux, en fonction de la menace perçue et de l'environnement de la cible.

3.2 Mode Actif : description

Le mode actif utilise la *sonde*, le *filtre* et l'*ampli de puissance* afin de générer un fort niveau sonore correspondant aux signaux audio du champ électrique détectés par la sonde. Si la sonde détecte un signal audio issu d'un microphone amplifié, le système produira alors un effet de bouclage acoustique comparable à l'effet *Larsen* produit par un amplificateur de sonorisation dont le gain serait trop élevé. Ce son strident est très caractéristique.



3.3 Avantages du mode Actif.

- a) Le mode Actif est le mode opératoire le plus facile d'utilisation.
- b) Il est plus rapide que le mode Passif.
- c) Il est plus sensible que le mode passif dans les mains de la plupart des opérateurs.

3.4 Inconvénients du mode Actif.

- a) Le fort niveau de son produit peut alerter le poste d'écoute qu'une recherche est en cours.
- b) Le niveau sonore empêche toute utilisation dans un environnement de travail normal en présence du personnel.
- c) Il est plus sujet à de fausses réponses que le mode passif.

3.5 Mode passif : description.

Lors d'une opération en mode Passif, l'unité *Amplificateur de Puissance* n'est pas employée. La *Sonde* est connectée au *Filtre*, et l'opérateur utilise le casque audio connecté au filtre afin d'écouter les bruits de la pièce détectés par un système de microphone espion.



3.6 Avantages du mode Passif.

- a) Une recherche menée correctement en mode passif n'alertera pas le poste d'écoute qu'une recherche est en cours, sans déranger le personnel présent dans les bureaux.
- b) Il est moins sujet à de fausses réponses que le mode actif.

3.7 Inconvénients du mode Passif.

- a) Un bon contrôle nécessite plus de temps que pour le mode Actif.
- b) Il est légèrement moins sensible que le mode actif.

4. Performances du système.

4.1 Les performances du système *BloodHound* dépendent des facteurs suivants :

- a) **Le niveau des émissions du champ électrique engendré par le matériel d'interception.** Le *BloodHound* est généralement efficace pour des systèmes à micro filaire qui ont un niveau de sortie suffisant pour permettre l'utilisation de câbles à paires torsadées. Cela comprend les microphones filaires utilisés par la plupart des services de renseignement mondiaux (mais pas tous). Le *BloodHound* n'est généralement pas efficace sur des équipements à faible niveau de sortie utilisant des câbles blindés.
- b) **Le niveau de blindage des microphones espions.** Le rayonnement du champ électrique peut être réduit par l'effet de blindage des matériaux se trouvant entre le microphone et la sonde du *BloodHound*. Les écrans métalliques, le béton, les châssis de fenêtres en métal, et le plâtre humide atténuent le signal du champ électrique dans une certaine mesure.
- c) **Le niveau du bruit ambiant.** Aux fréquences audio auxquelles opère le *BloodHound*, dans n'importe quel environnement est présent un bruit naturellement créé par le champ électrique augmenté du bruit électrique généré par l'homme.

4.2 Sensibilités typiques.

Les capacités du *BloodHound* à détecter les systèmes d'écoute sont soumis aux facteurs énumérés ci-dessus. Ci-dessous sont listées des exemples de détections caractéristiques basées sur des retours d'expérience du terrain.

- a) Microphone filaire sur une ligne à paires torsadées. D'une détection nulle pour un câble enterré profondément dans du béton, à une détection d'une portée de trois mètres pour une ligne insérée dans un châssis de porte en bois (mode passif).
- b) Microphone Radio. Double modulation avec masquage dans le bruit. 25 cm en Actif : 20 cm en Passif.
- c) Enregistreur à cassette. Déclenchement à la voie activé : 25 cm en Actif. 20 cm en Passif.
- d) Caméra vidéo. Signal vidéo détectable à un mètre (mode passif).

4.3 Remarquons que tous les cas précédents peuvent varier en fonction de l'environnement de recherche. Notons aussi les différences importantes dans la gamme de détection du microphone cité au § a) ; en effet il passe de réellement indétectable à « immanquable » en raison uniquement de la méthode de câblage vers le poste d'écoute.

4.4 La détection de systèmes espions par le *BloodHound* nécessite une recherche consciencieuse couvrant tous les emplacements possibles de dissimulation dans le volume de recherche, ainsi qu'une interprétation fine et réfléchie des résultats obtenus.

5. Optimisation de l'environnement de recherche

5.1 Bruit ambiant électrique

Il est nécessaire, autant que possible, de minimiser le bruit électrique car celui-ci réduira la sensibilité de l'ensemble *Bloodhound*. Bien que peu de choses peuvent se faire sur le bruit naturel (provenant principalement du soleil) le bruit technologique du à l'homme peut être diminué par la coupure des lampes fluorescentes et des moniteurs d'ordinateur, ainsi que tout ce qui pourrait s'avérer être gênant.

Dans le milieu domestique, il convient de noter que les systèmes HI-FI et la télévision peuvent considérablement produire du bruit électrique. Le mieux étant alors de les éteindre (mais sans les débrancher). Il est à noter que parfois des lampes fluorescentes éteintes génèrent plus de bruit qu'en fonctionnement de par les courants de fuite des câbles des vieux bâtiments.

5.2 Bruit ambiant acoustique

Contrairement au bruit électrique, effectuer une recherche avec le *BloodHound* nécessite autant de signaux sonores que possible dans l'environnement de recherche. Pour que le niveau du champ électrique créé par le microphone soit élevé, il est nécessaire que le niveau sonore capté par le micro soit important.

Une radio peut constituée une bonne source sonore. Localement un bruit peut être produit en tapant ou soufflant aux endroits suspects ce qui produira un niveau de sortie élevé de la part de microphones à proximité aux dépens d'une possible alerte du poste d'écoute.

PLUS IL Y A DE BRUIT DANS LES LOCAUX CONTROLES, MIEUX CELA SERA !

6. Fausses réponses

6.1 En plus des émissions provoquées par des systèmes de microphones filaires, des champs électriques de fréquences audio correspondants aux bruits de la pièce peuvent être générés par des matériaux isolants qui peuvent vibrer. Il s'agit notamment des sacs en plastique, des couvercles en plastique des téléphones et téléviseurs, papier, etc.

6.2 Bien que cet effet soit accentué dans le mode opératoire actif où le niveau sonore élevé peut amener de nombreuses surfaces à vibrer, cet effet est aussi perceptible en mode passif lorsque les objets plastiques sont légèrement tapotés.

6.3 Il est à noter que bien que tapoter le boîtier d'un téléphone peut très bien causer une fausse réponse à la sonde du *Bloodhound* tenue à proximité du cordon de ligne téléphonique, celui-ci est actif étant connecté à la ligne. L'expérience de l'utilisateur est le meilleur moyen d'identifier les réponses réelles des fausses.

6.4 Il est possible, mais peu probable, que des émetteurs de radiodiffusion de forte puissance puissent être détectés par le système *Bloodhound*. Il est fort probable, cependant, que soient détectés des émetteurs de radiodiffusion par les jonctions de semi-conducteurs présents dans les locaux ciblés par la recherche. Ces jonctions peuvent être dues à la corrosion des contacts dans les boîtiers électriques, des crochets de téléphones, ou des renforts de câbles dans les murs. Dans tous les cas, l'effet donne lieu à l'écoute d'une émission radio dans une petite zone localisée. Gardez à l'esprit qu'un système espion éteint peut également donner ce genre de réponse, ainsi ce phénomène mérite au moins une recherche visuelle.

6.5 Tenir l'antenne sonde à côté de la prise casque du filtre, ou à côté du haut-parleur de l'amplificateur de puissance peut provoqué un début de bouclage acoustique causé par des émissions de champs électriques à ces endroits. Ceci est utile pour vérifier la sensibilité du système.

7. Techniques de recherche

7.1 Critères pré requis

Cette section est écrite en supposant que l'opérateur est qualifié dans la conduite d'Opérations de Sécurité Electronique. Si ce n'est pas le cas, contactez votre distributeur pour de plus amples informations.

7.2 Méthode

Dans les deux modes actif ou passif, une recherche nécessite que la sonde soit déplacée sur toutes les surfaces qui pourraient dissimuler un système d'écoute. En mode passif, la recherche exigera une source sonore inoffensive telle qu'une radio produisant un stimulus pour le microphone depuis le centre de la pièce. Le volume de la radio devra être suffisamment fort sans gêner le voisinage. En mode actif, l'amplificateur de puissance devra être positionné face aux surfaces balayées ou face au mur à quelques mètres de celui-ci relié au filtre par un câble d'extension.

Dans les deux cas, le niveau d'éclairage de la zone de recherche doit être élevé, afin de permettre à l'opérateur de tirer pleinement parti d'un autre outil de l'opérateur de sécurité électronique : ses yeux.

L'antenne fixe de la sonde agit comme une antenne longue mais n'accroît pas la sensibilité, et peuvent être sujettes à la surcharge à la fois d'alimentations et d'émetteurs de radiodiffusion locaux. La sonde peut être montée sur un bras télescopique permettant une meilleure couverture avec facilité.

Même si vous avez l'intention d'effectuer un balayage en mode actif, utiliser en premier une recherche en mode passif. Même si cela ne concerne que les postes clés tels que les téléphones. Une recherche en mode passif peut identifier un système espion avant que le poste d'écoute ne réalise qu'une investigation est en cours.

Le niveau sonore produit par le mode actif peut causer des lésions pour les oreilles non protégées sur une longue période de temps. Le casque audio et la protection auditive fournie conviennent à une équipe d'inspection de deux hommes.

UTILISER LA PROTECTION AUDITIVE !

Probablement la méthode la plus efficace d'obtenir un niveau important d'un microphone est de souffler de l'air dessus. Cette méthode est très bien réalisée en utilisant la pompe photographique (nettoyage d'objectifs) fournie. L'efficacité réalisée par cette approche est très élevée, mais extrêmement localisée, et libre de toute possibilité d'une fausse réponse. Méfiez-vous des aérosols sous pression utilisant du fréon car celui-ci peut exercer une forte charge électrique créant du bruit dans les écouteurs du BloodHound.

8. Technologie

8.1 Sonde

La sonde est un filtre amplificateur à haute impédance. L'antenne de la sonde réalise efficacement le couplage avec le système espion. La sonde a une bande passante de 1 KHz à 20 KHz et atténue les signaux basses fréquences de 40 db/Décade.

La sonde est alimentée par le filtre via un câble coaxial et nécessite 5 mA pour une tension de 24 à 30V.

8.2 Filtre

La sortie de la sonde passe par un compresseur qui optimise le niveau du signal pour le reste du circuit de traitement de signaux.

La sortie du compresseur alimente un filtre récuratif, filtre à peigne, dont la réponse au 50 Hz ou au 60 Hz dépend de la position de l'interrupteur interne *Null*. Le filtre récuratif élimine toutes les harmoniques de l'alimentation secteur.

La sortie du filtre récuratif alimente la prise de sortie, et via le contrôle de volume du casque, à la prise casque du filtre.

Le filtre contient l'alimentation électrique de la sonde qui fournit le 26 VDC à une impédance de source de 600 Ohms, polarité positive au centre du coaxial.

8.3 Amplificateur de puissance

L'amplificateur de puissance a une efficacité de 4 W R.M.S. pour une charge de 4 Ohms, ou une tension de 12 V c-c pour la sortie B.N.C. jusqu'à 1 Ampère R.M.S. La sortie est protégée contre les courts-circuits.

Le générateur de tonalité interne produit un signal sonore sinusoïdal balayé entre environ 1 et 5 KHz. Le taux de balayage est variable d'environ 1 à 5 balayage/seconde par l'intermédiaire du contrôle de *Sweep Rate*.

L'amplificateur de puissance inclut des batteries gel rechargeables scellées et un circuit de charge permettant une utilisation continue pendant quatre heures. La mise en charge est automatique lorsque l'amplificateur est connecté au secteur, et les batteries ne peuvent être en surcharge.

9. Traceur de lignes

- 9.1** Le système *BloodHound* peut être utilisé pour tracer des lignes en connectant la sortie de l'amplificateur de puissance au câble à tracer, en positionnant les interrupteur sur *Output* et *Switch*, et en suivant le câble avec l'ensemble sonde/filtre tout en écoutant le son caractéristique du générateur audio de l'unité amplificateur.
- 9.2** Cette méthode de traçage de ligne diffère de la plupart des autres en raison de l'utilisation de basses fréquences, le signal a tendance à rester sur le câble désiré, et à ne pas passer sur les fils voisins.
- 9.3** Utiliser le contrôle de volume pour ajuster un niveau de signal approprié à l'opération de traçage.

10. Illumination de câbles

- 10.1** Il est possible de localiser et tracer des câbles dissimulés par induction au moyen d'une antenne émettrice connectée à la sortie de l'amplificateur de puissance. Une antenne à boucle d'induction appropriée est actuellement disponible auprès de Shearwater 2000.

11. Spécifications

11.1 Dimensions physiques

Sonde 5cm x 3cm x 11cm
Filtre 10cm x 6.5cm X 17.5cm
A.P. 21cm X 13cm X 16.5cm

12. Entretien régulier et réglages

- 12.1** Cet équipement ne requière pas d'entretien régulier ni de réglages. Si un défaut est remarqué, l'équipement doit être retourné à Shearwater 2000 ou à une installation de maintenance locale Shearwater 2000 pour réparation.