Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

C A H I E R N° 3

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

FOURNITURE D'ÉQUIPEMENTS INFORMATIQUES ET ÉLECTRONIQUES FORENSIQUES ET DE LUTTE CONTRE LA CYBERCRIMINALITÉ

FSI Fonds Sécurité Intérieure
Union européenne
l'Europe se mobilise

Le présent CCTP comporte 26 feuillets (numérotés de 1 à 26).

Sommaire

Suivi des modifications :
- le 09/11/18 : modification du 1.4.4

A- CONTEXTE

Le projet de marché de « **Fourniture d'équipements informatiques et électroniques de lutte contre la cybercriminalité** », @CYBERCRIME, a démarré en 2009 avec comme objectif de répondre aux besoins de fourniture de l'ensemble des matériels et des progiciels nécessaires aux investigations et aux enquêtes dans le domaine de la cybercriminalité.
Adhérant aux évolutions technologiques et à l'utilisation croissante de l'informatique, des smartphones et des réseaux sociaux en matière criminelle, le Ministère de l'Intérieur dispose aujourd'hui d'enquêteurs spécialisés en matière de lutte contre la cybercriminalité et l'investigation forensique, déployés sur l'ensemble du territoire national et outre-mer.
La Police et la Gendarmerie Nationales ont structuré un dispositif multi-niveaux au cœur duquel agissent les investigateurs en cybercriminalité (ICC), les enquêteurs technologies numériques (NTECH) et les spécialistes de la Police Technique et Scientifique. Ils bénéficient de formations de haut niveau validées par des équivalences universitaires. Ils reçoivent un équipement spécifique nécessaire à l'accomplissement de leurs missions.

B- GENERALITES

Documentation et support
La documentation associée est fournie en même temps que les équipements pour permettre à l'Administration d'exercer pleinement et de manière autonome :

- le paramétrage et la mise en ordre de marche des équipements livrés ;
- l'emploi des équipements livrés.

Les systèmes d'exploitation et les pilotes sont livrés impérativement sur un support numérique amovible ou par téléchargement sur Internet.

Câbles
Tous les équipements sont fournis avec les câbles adaptés et nécessaires à leur bon fonctionnement sur les sites de l'Administration.

Conformité des matériels
Les équipements fournis dans le cadre de l'exécution du présent accord-cadre sont des équipements neufs et conformes aux normes françaises et européennes en vigueur.

LOT 1 : MATERIELS D'INVESTIGATIONS FORENSIQUES

Dispositions générales :
Le prestataire propose toutes mises à jour, mineures ou majeures, du firmware par téléchargement, via Internet, pendant la durée de commercialisation des matériels.

1.1 : BLOQUEURS EN ÉCRITURE

L'investigation sur des supports numériques présuppose que ceux-ci soient verrouillés en écriture afin de préserver l'intégrité des pièces à conviction analysées. Pour ce faire, des bloqueurs matériels en écriture, disposés entre le support à examiner et l'ordinateur d'investigation, sont utilisés. Ils doivent être adaptés au type de support à analyser (IDE, SATA, SAS, FireWire ou USB).
Tous les bloqueurs sont livrés avec la connectique permettant de les relier au support à examiner.

Les bloqueurs doivent :

- permettre à l'enquêteur de préserver l'intégrité de la preuve numérique ;
- permettre à l'enquêteur d'accéder aux données en temps réel ;
- s'interfacer avec les différentes connectiques existantes (cf tableau) ;
- disposer d'un témoin de fonctionnement (ordinateur-hôte, disque dur et blocage en écriture) ;
- outrepasser la fonction HPA (Host Protected Area) de la norme ATA ;
- disposer d'un système de marche / arrêt.

L'Administration souhaite que les bloqueurs proposés disposent :

- d'un support pour le disque source ;
- d'un refroidissement du disque source ;
- d'un mécanisme simulant l'écriture de donnée sur le disque dur.

Tableau récapitulatif des bloqueurs

Types de bloqueurs	Connectique côté support à protéger	Connectique côté ordinateur	Portabilité
1.1.1 : Bloqueur pour disque dur IDE/SATA	IDE, SATA natif (sans adaptateur)	USB 3.0	Oui
1.1.2 : Bloqueur pour disque dur SAS	SAS natif (sans adaptateur)	USB 3.0	Oui
1.1.3 : Bloqueur pour périphériques de stockage USB	USB 1.0 et USB 2.0 minimum(Tout USB classique	USB 3.0	Oui
1.1.4 : Bloqueur pour périphériques de stockage FireWire	Firewire 400, Firewire 800	**USB 2.0 mini**	Oui
1.1.5 : Bloqueur pour disque dur IDE/SATA/SAS/Fire Wire 400 et 800/USB 3.0	IDE/SATA/SAS/FireWire 400 et 800/USB 3.0	USB 3.0	Intégration en baie 5’25’’

1.1.6 : Adaptateurs SSD et SSD M2 pour bloqueur 1.1.1

Ces adaptateurs permettent la connexion aux disques de stockage à tout format SSD incluant le M2.
Note : Les bloqueurs en baie incluent la connectique de branchement en interne d’une longueur suffisante.

1.1.7 : Système de blocage et de simulation en écriture

Il s'agit d'un système permettant aux enquêteurs de visualiser le contenu de l’ordinateur d'un suspect directement sur la machine en question, en temps réel, sans avoir à lancer d’acquisition du disque dur au préalable et sans outils de prévisualisation. Toutes ces opérations sont effectuées de manière forensique, sans altérer la preuve.

Concrètement, il s’agit d’un système de verrouillage en écriture qui s’intègre entre une carte mère et le disque dur (IDE ou SATA). Il permet de démarrer l’ordinateur suspect directement sur son système d’exploitation. Il est alors possible de naviguer dans le même environnement que le suspect, de lancer des recherches ou des applications et d'identifier des éléments de preuve, sans altérer l'intégrité des documents examinés.

Toutes ces opérations peuvent être effectuées sans aucune modification des données contenues dans l'ordinateur puisque le bloqueur bénéficie d'un disque dur interne qui va recueillir et bloquer toute tentative d'écriture lancée sur le disque suspect. Les écritures nécessaires au démarrage de l'ordinateur se font sur le disque dur du bloqueur qui permet la simulation d'une séquence de démarrage normal du système. Ce système permet le lancement du système d'exploitation et l'accès au contenu de l'ordinateur alors que tout son contenu reste verrouillé en écriture. Ce disque dur interne peut également être effacé de manière rapide grâce à un bouton dédié.

Ce type de système permet de présenter la preuve de manière claire et compréhensible pour les non-initiés. Il peut également être utilisé comme un outil de présélection permettant de se faire une idée rapide du contenu d'un disque dur et ainsi organiser le traitement des médias à analyser.

1.2 : DUPLICATEURS FORENSIQUES

Les duplicateurs forensiques doivent :

- détecter et désactiver HPA et DCO ;
- permettre à l'agent de préserver l'intégrité de la preuve numérique ;
- réaliser une copie fidèle (image et clone) du ou des supports à investiguer ;
- s'interfacer avec les différentes connectiques existantes (cf tableau) ;
- proposer une interface intuitive pour la manipulation par l'agent ;
- permettre un formatage, un effacement sécurisé, hash (MD5 ou SHA-1) ;
- permettre un usage discret, silencieux, avec coupure de l'écran lumineux (uniquement pour le duplicateur discret (1.3.3)) ;
- copier depuis un réseau (uniquement pour le duplicateur discret (1.3.3)).

L'Administration souhaite que les duplicateurs puissent :

- permettre une prévisualisation du contenu du disque, directement sur le duplicateur ;
- s'interfacer avec des connectiques supplémentaires ;
- copier depuis un réseau.

Tableau récapitulatif des duplicateurs

Usages	Copie	Disques durs	Discrétion	Rapidité	Acquisition réseau	Autre
1.2.1 : Duplicateur standard	1 vers 1	IDE/SATA/USB	-		-	**SAS a minima via un adaptateur**
1.2.2 : Duplicateur standard + SAS	1 vers 1	IDE/SATA/USB/SAS	-		-	-
1.2.3 : Duplicateur discret	1 vers 1		**oui**	**oui**	**oui**	-
1.2.4 : Duplicateur standard double copie	1 vers 2	IDE/SATA/USB	-		-	-
1.2.5 : Duplicateur copie de masse	2 vers 2 2 vers 4	IDE/SATA/USB	-		-	-
1.2.6 : Duplicateur disque dur sans démontage	1 vers 1, sans démontage	IDE/SATA/USB	-		-	**connectiques adaptées aux différentes sources** (inclus Apple)

1.2.7 : Adaptateurs SSD et SSD M2 pour duplicateur 1.2.1

Ces Adaptateurs permettent la connexion aux disques de stockage à tout format SSD incluant le M2.

LOT 2 : PROGICIELS D'INVESTIGATION NUMÉRIQUE ORIENTÉS TERRAIN

2.1 : ACQUISITIONS DE LICENCES

D’un point de vue des licences, les progiciels doivent :

- pouvoir être installés sur des micro-ordinateurs sous Windows ;
- avoir une interface graphique ;
- être de la version la plus récente incluant les mises à jour mineures et majeures (correctifs et montées de version) ;
- être livrés dans leur version complète (toutes fonctions actives et non bridées) ;
- être livrés avec un an de mise à jour incluse ;
- posséder une documentation au format électronique ou au format papier en français ou à défaut impérativement en anglais (une par licence) ;
- pouvoir être téléchargés sur Internet ou livrés sur un support numérique amovible.

2.1.1 : Progiciel d'investigation numérique orienté terrain, sans capacité de virtualisation

Ce progiciel intègre au minimum les fonctions suivantes :

- exécution depuis une clé USB ou un disque dur externe sans perte de fonctionnalités ;
- disponibilité en version 32 ou 64 bits ;
- réalisation d'images-disques au minimum aux formats DD et E01 ;
- possibilité de copier le support dans les deux sens du début à la fin ou de la fin vers le début ;
- possibilité d’exporter les données dans container ;
- lecture des systèmes de fichiers suivants : NTFS, FAT, HFS, EXT et XWFS ;
- utilisation d'un moteur d’indexation ;
- reconstruction des systèmes RAID ;
- accès à la RAM sur un système allumé (live) ;
- recherche de données au niveau binaire (carving) ;
- exécution de scripts personnalisés ;
- livré avec un pack d'afficheurs (viewers) et une visionneuse de fichiers vidéo ;
- calcul du pourcentage de couleur assimilable à la couleur de la chair dans une image (skin ton) ;
- analyse d’un document par rapport à la valeur de hash de ses parties (fuzzy doc) ;
- capacité à personnaliser les traitements d’analyse sur le support et pouvoir commencer à exploiter le support avant traitement.

2.1.2 : Progiciel d'investigation numérique orienté terrain, doté de capacité de virtualisation

Ce progiciel permet l’analyse d’un fichier d’image disque ou d’un support numérique derrière un dispositif matériel de blocage en écriture.

Les fonctionnalités obligatoires attendues sont les suivantes :

- virtualisation du système analysé : démarrage du système analysé dans une machine virtuelle sans altérer l'image disque ou le support analysé ;
- prise en charge des volumes chiffrés dont le mot de passe ou la clé de secours sont connus ;
- support des principaux systèmes de fichiers actuellement rencontrés (FAT 12/16/32, exFAT, NTFS, HFS, HFS+, EXT 2/3/4, CD/DVD ISO et UDF) et être en mesure de reconstruire un système RAID ;
- vérification du type de fichier ;
- gestion de bases de hash ;
- filtres ;
- visualisation du contenu des formats de fichiers les plus rencontrés ;
- déconstruction de containers ;
- recherche par mots clés et indexation.

Les fonctionnalités souhaitées sont les suivantes :

- scripts pour automatiser certaines tâches ou décoder des formats de fichiers non supportés ;
- analyse simplifiée des volumes Shadow Copy sous Windows.

2.2 : MISES À JOUR DE LICENCES

Conditions générales :

Les mises à jour prennent en compte les dernières évolutions progicielles et ou matérielles associées, mineures et majeures, relatives au produit initial.
Il s'agit d'une prestation annuelle.
Les mises à jour sont téléchargeables à distance (Internet, site de l'éditeur, etc.).

Les mises à jour suivantes sont attendues :

- 2.2.1 : Progiciel d'investigation numérique orienté terrain, sans capacité de virtualisation (§2.1.1)

- 2.2.2 : Progiciel d'investigation numérique orienté terrain, doté de capacité de virtualisation (§2.1.2)

2.3 : FORMATION RELATIVE AU PRODUIT 2.1.1

Les formations sont dispensées à des groupes de 10 personnes maximum.
Elles sont dispensées en français.
Elles ont lieu :

- dans les locaux et sur le matériel du prestataire ;
- sur le matériel du prestataire ou de l'Administration, dans les locaux de l'Administration :
    - en Île-de-France ;
    - en province ;
    - en outre-mer.

Un support pédagogique papier ou numérique, en français de préférence ou à défaut en anglais, est remis à chaque stagiaire en début de la formation. Ce support pédagogique doit être suffisam-

ment étayé pour permettre au stagiaire de se réapproprier sa formation longtemps après celle-ci. Il est donc acquis de façon définitive par le stagiaire.
Chaque jour de la formation, le prestataire fait émarger la feuille de présence aux stagiaires. A l'issue de la formation, le prestataire fait remplir au stagiaire un formulaire d'évaluation du stage. A l'issue du stage, les deux documents, feuille de présence et formulaire d'évaluation, sont transmis par le prestataire à l'Administration.
A l'issue de sa formation, le stagiaire doit être capable de mettre en œuvre les matériels et progiciels sur lesquels il a été formé.

LOT 3 : PROGICIELS D'INVESTIGATION NUMÉRIQUE ORIENTÉS LABORATOIRE

3.1 : ACQUISITIONS DE LICENCES

D’un point de vue des licences, les progiciels doivent :

- pouvoir être installés sur des micro-ordinateurs sous Windows ;
- avoir une interface graphique ;
- être de la version la plus récente incluant les mises à jour mineures et majeures (correctifs et montées de version) ;
- être livrés dans leur version complète (toutes fonctions actives et non bridées) ;
- être livrés avec un an de mise à jour incluse ;
- posséder une documentation au format électronique ou au format papier en français ou à défaut impérativement en anglais (une par licence) ;
- pouvoir être téléchargés sur Internet ou livrés sur un support numérique amovible.

PROGICIELS FORENSIQUES DE RECHERCHE ET D’ANALYSE DE DONNEES

3.1.1 : Progiciel d'acquisition de données pour produits Mac

Ce progiciel doit :

- être basé sur une architecture MAC ;
- acquérir des systèmes de fichiers MAC, même les plus récents.

Les fonctionnalités souhaitées sont les suivantes :

- disposer de fonction de triage ;
- détecter un chiffrement natif MAC.

3.1.2 : Progiciel d’analyse de données pour produits Mac

Ce progiciel doit :

- rechercher et analyser les données, effacées ou non, contenues dans un ordinateur Mac ;
- acquérir des systèmes de fichiers MAC, même les plus récents ;
- créer des images-disques forensiques (copie binaire) directement depuis une clé bootable contenant ce progiciel.

L’Administration souhaite que le progiciel puisse virtualiser le système analysé.

3.1.3 : Analyse et récupération de données effacées sur bases SQLite

Ce progiciel ou cette suite de progiciels permet l'affichage, l'analyse et la récupération de données effacées d'une base SQLite.

PROGICIELS D'ANALYSE DE FICHIERS TEXTES

3.1.4 : Progiciel d'aide à la rédaction d'expressions régulières

Ce progiciel doit :

- permettre de créer des expressions régulières complètes répondant aux spécifications de l'enquêteur sans que celui-ci ait besoin de connaître précisément la syntaxe ;
- permettre à l'enquêteur de se contenter de fournir au progiciel des extraits de textes ou des formats de chaîne de caractères (N° de téléphone, de carte bancaire, d'immatriculation, etc) qu'il souhaite trouver pour que le progiciel génère automatiquement l'expression régulière correspondante.

3.1.5 : Progiciel d'analyse et de développement d'expressions régulières

Ce progiciel doit :

- permettre de comprendre des expressions régulières complexes écrites par d'autres personnes, de les tester pour s'assurer de leur validité et au besoin, de les corriger afin de les faire correspondre au besoin, sans avoir à procéder par tâtonnement ;
- permettre d'alimenter une bibliothèque d'expressions régulières pour une réutilisation ultérieure.

3.1.6 : Progiciel d'exploitation d'expressions régulières

Ce progiciel doit :

- permettre la mise en œuvre d'expressions régulières pour rechercher une chaîne de caractères dans un grand nombre de fichiers sur un PC ou un réseau et notamment dans :
  - des fichiers textes et binaires ;
  - des archives compressées ;
  - des documents MS Word ;
  - des tableurs Excel ;
  - des fichiers PDF ;
  - des fichiers OpenOffice ;
- présenter les résultats de la recherche sous forme d'une liste ;
- afficher rapidement un aperçu ;
- ouvrir un fichier dans lequel l'expression a été trouvée ;
- mettre en évidences les expressions régulières dans le fichier ouvert afin de faciliter le contrôle du contexte des occurrences trouvées.

3.1.7 : Progiciel éditeur de texte professionnel

Ce progiciel doit :

- ouvrir de nombreux fichiers texte en même temps, sans limitation de volume ;
- organiser les fichiers textes en multiples projets pour les ouvrir en une fois et les éditer ensemble ;
- ouvrir tous les fichiers d'un dossier (et de ses sous-dossiers) dans un projet ;
- exécuter des commandes d'édition sur tous les fichiers d'un projet en même temps ;
- basculer rapidement entre les dossiers et les projets en cliquant sur leurs onglets ;
- gérer de longues listes de fichiers texte et de grands projets grâce à une interface graphique qui permet de renommer, de déplacer, de copier et de supprimer des fichiers ;
- rechercher et remplacer du texte automatiquement ;
- utiliser des fonctions de coloration syntaxiques ;
- comparer 2 fichiers texte (notamment surligner les différences, fusionner les 2 fichiers, extraire les similitudes et les différences) ;
- lister des fichiers, les trier par ordre alphabétique et supprimer les doublons ;
- utiliser des fonctions de statistiques pour voir instantanément le nombre de paragraphes, de mots et de lettres d'un fichier ;
- ouvrir des fichiers texte enregistrés avec des ordinateurs sous Linux, UNIX et Mac ou avec d'anciens systèmes tels que PC sous DOS ou IBM.

PROGICIELS RELATIFS AUX MAILS

3.1.8 : Récupérateur d'e-mails

Ce progiciel doit :

- comprendre plusieurs formats de mails atypiques ;
- convertir et exploiter au minimum les formats suivants d'emails et newsgroups : Outlook, Outlook Express, AOL, Eudora, Pegasus, TheBat, Netscape, Mozilla Thunderbird et Mbox ;
- récupérer les emails considérés comme effacés par le client de messagerie mais encore présents dans le fichier d'archive de messagerie.

3.1.9 : Traducteur de formats d'e-mails

Ce progiciel doit comprendre plusieurs formats de mails atypiques et les transformer en formats classiques.

3.1.10 : Progiciel d'analyse et de croisement de mails et de données numériques disposant d'une capacité de visualisation graphique

Ce progiciel d'analyse de mails et de données numériques doit traiter un volume supérieur à 250 Go et prendre en charge le plus grand nombre possible de formats de mails.

Le progiciel doit traiter simplement les mails et les données numériques, visualiser les résultats sous un format graphique, identifier les relations et les données pertinentes et exporter les résultats vers une grande variété de format de fichiers.

PROGICIELS DIVERS

3.1.11 : Progiciel de collecte, de tri et d'analyse d'information sur Internet

Ce progiciel doit :

- mettre en évidence des liens entre différentes personnes, réseaux sociaux, sociétés, organisations, sites web, infrastructure Internet (nom de domaine, DNS, Netblocks, adresse IP), phrases, affiliations, documents et fichiers, en les affichant de façon très visuelle remplacer par graphique ;
- trouver les données personnelles en ligne d'un internaute (ses adresses e-mails, ses blogs, ses amis, ses préférences personnelles, sa localisation, sa description de poste, etc) ;
- affiner les résultats des recherches ;
- pouvoir travailler sur le graphique et supprimer les liens inopportuns ;
- pouvoir afficher plusieurs milliers de résultats par requête sur le graphique ;
- permettre de travailler jusqu'à plusieurs milliers de résultats par requête ;
- permettre de travailler sans limitation du nombre des requêtes ;
- pouvoir accéder à la source par lien cliquable.

3.1.12 : Progiciel étendu de collecte, de tri et d'analyse d'information sur Internet

Le progiciel doit permettre :

- la découverte de données à partir de sources ouvertes et la visualisation de ces informations sous forme de graphiques, adaptés à l'analyse de liens et à l'exploration de données ;
- d'analyser les relations réelles (réseaux sociaux notamment) entre les personnes, les groupes, les pages Web, les domaines, les réseaux, l'infrastructure Internet et les affiliations à des services en ligne tels que Twitter et Facebook ;
- de travailler notamment à partir d'adresses mail, de pseudonymes, de noms d'utilisateur et de numéros de téléphones ;
- de cartographier les éléments obtenus sous un format graphique modulable et interactif ;
- de pouvoir afficher plusieurs dizaines milliers de résultats par requête sur le graphique ;
- de travailler jusqu'à plusieurs dizaines de milliers de résultats par requête ;
- de travailler sans limitation du nombre des requêtes.

3.1.13 : Module compatible avec MALTEGO permettant d'améliorer les capacités de recherche

Ce module doit :

- être compatible avec MALTEGO ;
- permettre de cartographier un maximum de réseaux sociaux différents à travers un maximum de « transformations » complémentaires.

L'Administration souhaite que ce module puisse éditer un rapport automatique.

3.1.14 : Progiciel casseur de mot de passe

Ce progiciel doit afficher et sauvegarder le contenu en clair d'un fichier protégé par mot de passe et/ou chiffré, en découvrant un mot de passe compatible ou en exploitant une vulnérabilité du progiciel ayant servi à créer le fichier.

L'administration souhaite que ce progiciel dispose d'une interface graphique.

3.1.15 : Progiciel de virtualisation (hyperviseur de type 2)

Ce progiciel doit :

- créer ou exploiter une machine virtuelle ;
    - quel que soit le système d'exploitation de la machine de travail ;
    - en prenant en compte le maximum de systèmes d'exploitation pour les machines virtuelles, et à minima Windows et Linux ;
    - même avec des petites configurations matérielles de travail ;
- permettre les interactions entre la machine physique et la machine virtuelle ;
- figer l'état de la machine virtuelle à un temps donné (Snapshot).

3.1.16 : Progiciel étendu de virtualisation

Ce progiciel doit :

- créer ou exploiter une machine virtuelle ;
    - quel que soit le système d'exploitation de la machine de travail ;
    - en prenant en compte le maximum de systèmes d'exploitation pour les machines virtuelles, et à minima Windows et Linux ;
    - même avec des petites configurations matérielles de travail ;
- permettre les interactions entre la machine physique et la machine virtuelle ;
- figer l'état de la machine virtuelle à un temps donné (Snapshot) ;
- permettre la gestion simultanée de plusieurs machines virtuelles et la mise en réseau de celles-ci.

3.1.17 : Progiciel forensique d'analyse des données de navigation de GPS

Ce progiciel doit :

- prendre en charge, au minimum, les données de navigations des GPS suivants : TomTom, Garmin et Navman ;
- lire les données de localisation enregistrées et effacées des GPS TomTom et les fournira de façon horodatée ;
- lire tous les Waypoints et routes des GPS Garmin ;
- lire toutes les localisations et logs des GPS Navman ;
- lire les données téléphones et SMS des GPS TomTom et Navman ;
- faire des exports vers Google Earth ;

- afficher les résultats sur une cartographie intégrée ;
- exporter un rapport au format PDF.

3.1.18 : Analyseur de traces de navigateurs web orienté laboratoire

Ce progiciel doit :

- exploiter tous les formats suivants de traces de navigation Web : Internet Explorer (versions 3 à 10) pour Windows, Internet Explorer pour Mac, Netscape, Firefox (versions 1 à 18), Safari et Opera ;
- exploiter et visualiser à la fois les cookies, le cache et l'historique de navigation, tout en liant ces traces entre elles ;
- extraire ces traces quand elles sont effacées et présentes dans les secteurs non alloués d'un support numérique (ex : disque dur) ;
- offrir des possibilités de détection automatique des requêtes effectuées sur les moteurs de recherche les plus courants, de détection automatique des logins et mots de passe utilisés, de recherches par dates ou par mots-clés, de tri par ordre alphabétique ou chronologique, de tri par fréquence de visite, de filtrage automatique des fichiers images, vidéos et archives ;
- éditer des rapports d'analyse et de sauvegarder une analyse en cours.

3.2 : MISES À JOUR DE LICENCES

Conditions générales :
Les mises à jour prennent en compte les dernières évolutions progicielles et ou matérielles associées, mineures et majeures, relatives aux progiciels acquis.
Il s'agit d'une prestation annuelle.
Les mises à jour sont téléchargeables à distance (Internet, site de l'éditeur, etc.).

Les mises à jour suivantes sont attendues :

- 3.2.1 : Progiciel d'acquisition de données pour produits Mac (§3.1.1)
- 3.2.2 : Progiciel d'analyse de données pour produits Mac (§3.1.2)
- 3.2.3 : Analyse et récupération de données effacées sur bases SQLite (§3.1.3)
- 3.2.4 : Progiciel d'aide à la rédaction d'expressions régulières (§3.1.4)
- 3.2.5 : Progiciel d'analyse et de développement d'expressions régulières (§3.1.5)
- 3.2.6 : Progiciel d'exploitation d'expressions régulières (§3.1.6)
- 3.2.7 : Progiciel éditeur de texte professionnel (§3.1.7)
- 3.2.8 : Récupérateur d'e-mails (§3.1.8)
- 3.2.9 : Traducteur de formats d'e-mails (§3.1.9)
- 3.2.10 : Progiciel d'analyse et de croisement de mails et de données numériques disposant d'une capacité de visualisation graphique (§3.1.10)
- 3.2.11 : Progiciel de collecte, de tri et d'analyse d'information sur Internet (§3.1.11)
- 3.2.12 : Progiciel étendu de collecte, de tri et d'analyse d'information sur Internet (§3.1.12)
- 3.2.13 : Module compatible avec MALTEGO permettant d'améliorer les capacités de recherche (§3.1.13)
- 3.2.14 : Progiciel casseur de mot de passe (§3.1.14)
- 3.2.15 : Progiciel de virtualisation (hyperviseur de type 2) (§3.1.15)
- 3.2.16 : Progiciel étendu de virtualisation (§3.1.16)
- 3.2.17 : Progiciel forensique d'analyse des données de navigation de GPS (§3.1.17)
- 3.2.18 : Analyseur de traces de navigateurs web orienté laboratoire (§3.1.18).

LOT 4 : PROGICIELS DEDIES A LA RECUPERATION ET A L'ANALYSE DE TRACES INTERNET ORIENTES TERRAIN

4.1 : ACQUISITION DE LICENCE

Exigences communes aux nouvelles licences :
Les progiciels doivent :

- pouvoir être installés sur des micro-ordinateurs sous Windows ;
- avoir une interface graphique ;
- être de la version la plus récente incluant les mises à jour mineures et majeures (correctifs et montées de version) ;
- être livrés dans leur version complète (toutes fonctions actives et non bridées) ;
- être livrés avec un an de mise à jour incluse ;
- posséder une documentation au format électronique ou au format papier en français ou à défaut impérativement en anglais (une par licence) ;
- pouvoir être téléchargés sur Internet ou livrés sur un support numérique amovible.

4.1.1 : Analyseur de traces de services Internet orienté terrain

Ce progiciel doit :

- extraire d'un média de type disque dur ou d'une image de celui-ci, les artéfacts les plus courants de la navigation internet, ainsi que les artéfacts les plus courants de messagerie instantanée. Les données sont présentées sous un format facilement intelligible ;
- assurer la préservation de l'intégrité des données analysées ;
- être démarré depuis une clé USB sans avoir à être installé sur un ordinateur ;
- analyser un système en live comme dans en environnement de laboratoire ;
- rechercher par mot clés ;
- rechercher des traces de messagerie instantanée ;
- rechercher des traces d'utilisation de webmail et de réseaux sociaux ;
- rechercher des traces de partage de fichiers en ligne ;
- rechercher des traces dans les fichiers systèmes pagefile.sys et hiberfil.sys ;
- rechercher les traces susmentionnées dans les espaces non alloués ou effacés (carving) et ce, également dans :
  - des copie-images de supports numériques ;
  - des dumps de RAM ;
  - des captures PCAP ;
- vérifier automatiquement le chiffrement du disque dur (TrueCrypt, PGP, BitLocker et SafeBoot) ;
- monter et inspecter les volumes Shadows Copies ;
- créer des aperçus des documents ;
- éditer des rapports d'analyse et de sauvegarder une analyse en cours ;
- exporter les données vers HTML, PDF, XLS et CSV ;
- créer des dossiers portables.

4.1.2 : Module complémentaire au §4.1.1 pour artefacts des systèmes d'exploitation et applications professionnelles

Ce module complémentaire au progiciel du §4.1.1 permet la collecte et l'exploitation des artefacts liés au système d'exploitation et aux applications professionnelles.

4.1.3 : Module complémentaire au §4.1.1 pour mobile

Ce module complémentaire au progiciel du §4.1.1 extrait et exploite les données provenant des matériels mobiles les plus courants (smartphones et tablettes).

4.1.4 : Solution d'analyse de la navigation Internet possédant une capacité de visualisation graphique

Le progiciel doit :

- extraire d'un média de type disque dur ou d'une image de celui-ci les artéfacts les plus courants de la navigation internet, ainsi que les artéfacts les plus courants de messagerie instantanée ;
- présenter les données sous un format facilement intelligible et croisées entre elles ;
- permettre à l'enquêteur d'accéder rapidement aux données les plus pertinentes et les visualiser sous un format graphique pour une analyse plus efficiente ;
- accéder aux données provenant de Windows, linux ou USB ;
- établir les relations entre les artéfacts, les fichiers et les utilisateurs ;
- déchiffrer les supports chiffrés ;
- ajouter de nouvelles preuves au dossier ;
- examiner l'arborescence du système de fichier ;
- améliorer et simplifier la recherche en permettant un tri et un filtrage des données par mot clés, date, heure, balise ;
- permettre une recherche croisée sur le support (approche intégrées, artefacts connexes) ;
- permettre à l'enquêteur de créer son propre artéfact ;
- créer des aperçus (base SQLITE, système de fichier, fichier supprimé, registre) ;
- exporter les données au minimum aux formats HTML, PDF, XLS et CSV.

L'Administration souhaite que la fourniture du matériel soit accompagnée d'une notice en français et/ou d'une vidéo de prise en main de l'outil en français (démonstration).

4.1.5 : Module complémentaire au §4.1.4 pour l'informatique en nuage

Ce module complémentaire du progiciel du §4.1.4 doit, via l'usage de l'identifiant et du mot de passe ou via l'usage d'un artéfact présent dans le support analysé, récupérer à distance les informations contenues dans les principaux services cloud (Informatique en nuage).

4.1.6 : Module complémentaire au §4.1.4 permettant de traiter les systèmes mobiles

Ce module complémentaire du progiciel du §4.1.4 doit extraire et exploiter les données provenant des matériels mobiles les plus courants (smartphones et tablettes).

4.1.7 : Progiciel §4.1.4 et ses modules complémentaires des §4.1.5 et §4.1.6

4.2 : MISES À JOUR DE LICENCE

Conditions générales :
Les mises à jour prennent en compte les dernières évolutions progicielles et ou matérielles associées, mineures et majeures, relatives au produit initial.
Il s'agit d'une prestation annuelle.
Les mises à jour sont téléchargeables à distance (Internet, site de l'éditeur, etc.).

Les mises à jour attendues sont les suivantes :

- 4.2.1 : Analyseur de traces de services Internet orienté terrain (§4.1.1)
- 4.2.2 : Module complémentaire au §4.1.1 pour artefacts des systèmes d'exploitation et applications professionnelles (§4.1.2)
- 4.2.3 : Module complémentaire au §4.1.1 pour mobile (§4.1.3)
- 4.2.4 : Solution d'analyse de la navigation Internet possédant une capacité de visualisation graphique (§4.1.4)
- 4.2.5 : Module complémentaire pour l'informatique en nuage (§4.1.5)
- 4.2.6 : Module complémentaire permettant de traiter les systèmes mobiles (§4.1.6)
- 4.2.7 : Progiciel §4.1.4 et ses modules complémentaires des §4.1.5 et §4.1.6 (§4.1.7)
- 4.2.8 : Evolution du progiciel du §4.1.1 vers le progiciel §4.1.4 incluant la mise à jour du progiciel §4.1.4

LOT 5 : SOLUTION D'AIDE A L'INVESTIGATION PERMETTANT D'EXPLORER LE DEEPWEB ET LE DARKWEB

5.1 : ACQUISITIONS DE SOLUTIONS

Cette solution doit :

- créer un espace sécurisé permettant de travailler sans être directement sur les forums d'échange ;
- effectuer des recherches par mots clés et d'exporter ses résultats au minimum au format CSV ;
- collecter un maximum d'informations (notamment images, conversations) ;
- récolter et proposer au minimum des sources du french deep web ;
- proposer un mailing quotidien des informations ainsi découvertes en précisant leurs sources ;
- interroger une base d'adresse IP avec une possibilité de recherche par zone géographique.

5.2 : MISES À JOUR DE LA SOLUTION DÉFINIE EN 5.1

Les mises à jour prennent en compte les dernières évolutions progiciel les et ou matérielles associées, mineures et majeures, relatives au produit initial.
Il s'agit d'une prestation annuelle.
Les mises à jour sont téléchargeables à distance (Internet, site de l'éditeur, etc.).

LOT 6 : SYSTEMES D'EXTRACTION ET D'EXPLOITATION DE DONNEES PROVENANT DE SUPPORTS MOBILES

6.1 : ACQUISITIONS DE SYSTÈMES D'EXTRACTION ET D'EXPLOITATION DE DONNÉES PROVENANT DE SUPPORTS MOBILES

Les exigences communes aux systèmes sont les suivantes :

- exporter ces données sous un format facilement exploitable ;
- fournir une solution sans limitation d'usage permettant de lire cet export sur un ordinateur ;
- récupérer les SMS, les MMS, les historiques internet, le calendrier, le répertoire des contacts, les données des applications de messagerie, les journaux d'appels, les données de localisation et tous fichiers audio-image-vidéo-texte stockés sur le support ;
- limiter l'intervention de l'utilisateur pour un résultat sécurisé : un guidage simple et en français de l'utilisateur (flux des taches pré-établi) ;
- être accompagné de l'ensemble de la connectique nécessaire à l'extraction des données.

Au titre des références 6.1.1 et 6.1.2, le prestataire doit fournir 1 an de mises à jour du système et des connectiques (cf 6.3). Il fournit également un tutoriel vidéo en ligne en français.

6.1.1 : Système d'extraction et d'exploitation de données logiques provenant de supports mobiles via un protocole de travail sécurisé

En plus des exigences communes, le système doit extraire, le plus rapidement possible, les données au niveau logique sur le maximum de supports mobiles.

6.1.2 : Système d'extraction et d'exploitation de données physiques provenant de supports mobiles via un protocole de travail sécurisé

En plus des exigences communes, le système doit extraire, les données au niveau physique sur le maximum de supports mobiles.

6.2 : ACQUISITIONS SYSTÈMES D'EXTRACTION ET D'EXPLOITATION DE DONNÉES PROVENANT DE SUPPORTS MOBILES, INTÉGRÉS À UNE SOLUTION MATÉRIELLE

Données …	***… sur solution matérielle fixe***	***… sur solution matérielle mobile***
Logiques	*6.2.2*	*6.2.1*
Physiques	*Non applicable*	*6.2.3*

6.2.1 : Solution visée au §6.1.1 et intégrée dans une solution matérielle mobile

L'Administration souhaite extraire et analyser les données sur la même solution matérielle fournie. La solution matérielle doit disposer d'un port USB pour exporter sur un support numérique amovible le résultat de l'extraction.

6.2.2 : Solution visée au §6.1.1 et intégrée dans une solution matérielle fixe

La solution matérielle fixe est sécurisée. Elle est exclusivement dédiée à l'exécution du système fourni.
Cette solution matérielle doit disposer d'un port USB pour exporter sur un support numérique amovible le résultat de l'extraction.
L'Administration souhaite que l'interface soit tactile.

6.2.3 : Solution visée au §6.1.2 et intégrée dans une solution matérielle mobile

L'Administration souhaite extraire et analyser les données sur la même solution matérielle fournie. La solution matérielle doit disposer d'un port USB pour exporter sur un support numérique amovible le résultat de l'extraction.

6.3 : MISES À JOUR

Cette référence comprend la mise à jour du système et des solutions matérielles associées pour améliorer ses fonctionnalités d'extraction et d'analyse ainsi que de rendre le système compatible avec les nouveaux supports mobiles.
Les nouvelles connectiques nécessaires à l'extraction et à l'analyse sont fournies.

Les mises à jour suivantes sont attendues :

- 6.3.1 : Système d'extraction et d'exploitation de données logiques provenant de supports mobiles via un protocole de travail sécurisé (§6.1.1)
- 6.3.2 : Système d'extraction et d'exploitation de données physiques provenant de supports mobiles via un protocole de travail sécurisé (§6.1.2)
- 6.3.3 : Solution visée au §6.1.1 et intégrée dans une solution matérielle mobile (§6.2.1)
- 6.3.4 : Solution visée au §6.1.1 et intégrée dans une solution matérielle fixe (§6.2.2)
- 6.3.5 : Solution visée au §6.1.2 et intégrée dans une solution matérielle mobile (§6.2.3)