L'Internet des objets
à l'épreuve de la criminalistique numérique

Par François Bouchaud

La criminalistique numérique a été popularisée avec le développement et la diffusion des séries télévisées telles que NCIS ou « Les experts ». À ses débuts, elle résulte de demandes opérationnelles des Forces de Sécurité Intérieure (FSI), dans le cadre d'une enquête sur un crime impliquant l'appropriation du système informatique, généralement un ordinateur personnel, un téléphone portable ou un serveur. Cependant, les enquêtes médico-légales numériques ne se limitent pas aux affaires de cybercriminalité telles que l'accès ou sa tentative non autorisés à un système de traitement automatisé de données ou la diffusion de contenus d'exploitation sexuelle de mineurs. De plus en plus, elles sont également présentes dans des activités criminelles impliquant l'utilisation d'un appareil informatique ou numérique, comme dans les cas de trafic ou de blanchiment d'argent dans lesquels l'appareil numérique constitue le vecteur de l'infraction.

FRANÇOIS BOUCHAUD

Capitaine de Gendarmerie. Chef du département coordination du Centre de lutte contre les criminalités numériques (C3N).

À cette diversification du périmètre infractionnel et des usages s'ajoutent de nouveaux défis techniques. Le développement des écosystèmes connectés à Internet confronte la médecine légale à des dispositifs et des environnements hétérogènes, étendus et interconnectés avec de fortes dépendances. La donnée probante se retrouve fragmentée et dispersée au gré de la politique de gestion de la donnée, tant au niveau du stockage que de la synchronisation dans le réseau. Cette structuration de l'espace numérique et physique constitue donc un tournant dans l'analyse et la compréhension des phénomènes, nécessitant une contextualisation de la donnée et de sa diffusion.

Cependant, elle est gage d'opportunités inédites dans le recueil de données probantes par son fort ancrage dans l'environnement de l'utilisateur, tant dans la digitalisation de ses habitudes que dans le monitoring des systèmes.

1- Présentation d'une scène de crime connectée

Classiquement, les matériels étudiés sont des ordinateurs, des appareils mobiles, des passerelles, des équipements de stockage ou des serveurs. L'Internet des objets ouvre de nouvelles perspectives en introduisant des sources qui diffèrent par leur nature, leur nombre, leur format et les protocoles utilisés. Ainsi, les données probantes sont extraites ou proviennent des appareils ménagers, de systèmes domotiques, des équipements médicaux pour le vivant « homme ou animal », des voitures, des lecteurs RFID, *etc.* Par conséquence, les données sont plurielles et varient en fonction des interactions avec l'environnement et des services fournis. Pour illustrer ces propos et répondre aux multiples défis que génère la criminalistique dans l'Internet des objets, nous vous proposons d'étudier une scène de crime contenant des dispositifs intelligents et communicants.

Le 10 avril 2018, à 8 heures, le CORG[1] est alerté pour le cambriolage d'un

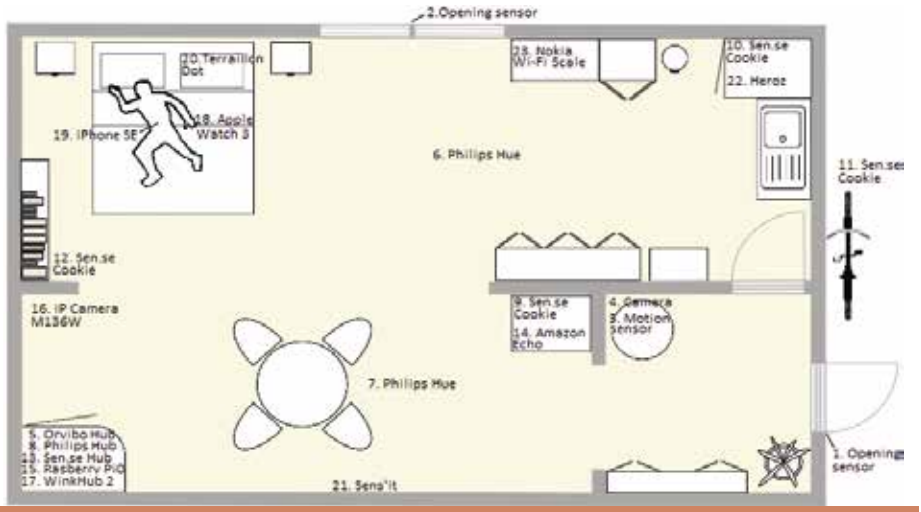

Figure 1 : croquis de l'appartement avec les équipements connectés.

(1) Centre d'opérations et de renseignement de la gendarmerie, niveau départemental.

appartement. Une patrouille de gendarmerie arrive à 8h15 sur le lieu des faits. Lors de la reconnaissance, elle découvre la porte d'entrée de l'appartement fracturée. Les premières constations font ressortir de nombreuses traces de lutte et de violence avec des objets renversés et brisés sur le sol. Dans une pièce, une personne décédée est retrouvée gisant sur un lit. La patrouille met donc en œuvre les premières mesures de protection de la scène de crime et demande un appui auprès des unités compétentes. Une équipe médico-légale, dont un technicien en nouvelles technologies, prend en charge la scène de crime à 9 heures. Il procède à l'appréhension de l'environnement en identifiant les différents objets connectés (figure 1) et en traçant la cartographie des interactions (figure 2).

L'appartement s'étend sur une surface de 45 m². Il comprend trois pièces distinctes : une entrée (pièce 1), une chambre (pièce 2) et un salon (pièce 3). Il est équipé d'un système domotique issu d'un kit *Orvibo*, avec deux capteurs d'ouverture (1 et 2) et un capteur de mouvement (3) couplé à une caméra Wi-Fi (4). Cette solution contrôle les deux ouvertures extérieures. Elle communique par le protocole *ZigBee* au travers d'une passerelle dédiée (5). Le système domotique est complété d'une ampoule Philips (6 et 7) connectée à sa passerelle (8). Par ailleurs, quatre capteurs *Sen.se Cookies* sont cachés dans les différentes pièces. Ils transforment les objets ménagers en objets connectés. Dans cette situation, ils surveillent la température ambiante de l'appartement (9), le niveau d'eau de la machine à café (10), la position du vélo en extérieur (11) et la gestion de la bibliothèque (12).

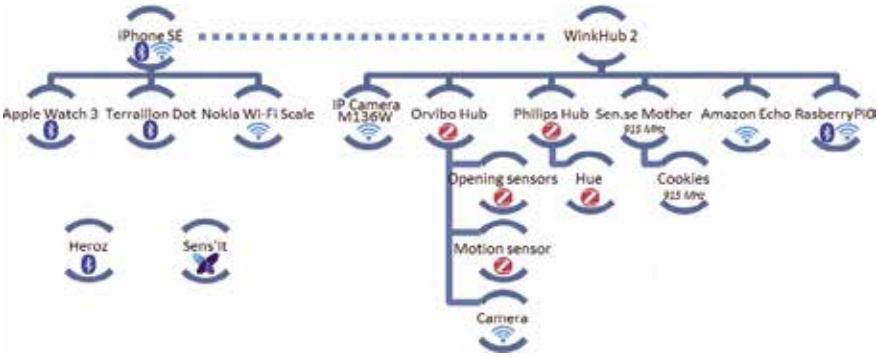

Figure 2 : cartographie globale de l'environnement local [1].

Tous ces équipements sont reliés à une base centrale *Sen.se Mother* et communiquent avec un protocole propriétaire (13). Les différentes passerelles *Orvibo, Philips et Sen.se, l'Amazon Echo* (14), le *RaspberryPi0* (15) et la caméra IP M136W (16) sont connectées à Internet au travers d'un *WinkHub* 2 (17).

La victime est allongée sur le lit de la chambre. Elle porte à son poignet droit une *Apple Watch* 3 (18) et a un *iPhone SE* (19) dans sa poche. Un capteur de sommeil *Terraillon Dot* (20) est caché dans le lit. D'autres objets hétéroclites sont disposés dans l'appartement : un *Sens'it* (21), un bracelet *Heroz* (22) et une balance *Nokia* (23).

2- Appréhension de l'environnement connecté dans sa globalité

Dans une démarche analytique de l'environnement, l'écosystème se découpe en trois zones complémentaires (figure 3) [2] : un environnement local composé des objets connectés et des passerelles (1), une infrastructure externalisée construite autour de plateformes Cloud (2) et un interfaçage avec l'utilisateur ou avec un autre système connecté (3). L'appréhension de la scène de crime se focalise sur l'environnement local, soit les zones 1 et 3. Seules les données de ces zones demeurent directement accessibles aux enquêteurs. L'acquisition des données de la zone 2 nécessite l'intervention d'un tiers, initiée par une réquisition judiciaire. Cependant, les demandes auprès des opérateurs de plateforme doivent

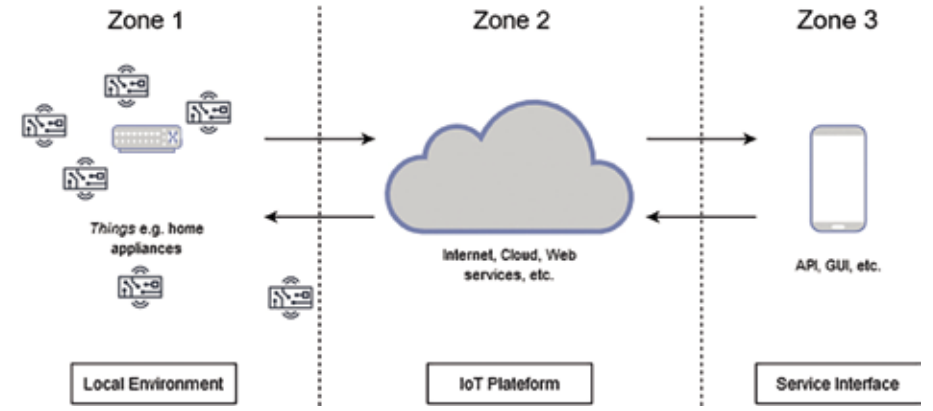

Figure 3 : découpage par zones de l'environnement connecté.

être orientées et motivées en fonction des informations recueillies localement, en particulier dans l'identification de l'équipement et des données remontées.

Chaque infrastructure est caractérisée par une politique de gestion de la donnée unique. Par exemple, le *Terraillon Dot* est synchronisé manuellement alors que l'*Apple Watch* utilise une synchronisation automatique. De même, la caméra *Orvibo* utilise un stockage externe comme mémoire tampon dans la communication avec le réseau. La donnée remontée se retrouve alors dispersée au sein du réseau au gré des configurations et des services proposés. Un équipement est susceptible d'être contrôlé ou accessible à partir d'un autre appareil du système, selon une structure de lien caché. La donnée se propage dans les équipements du réseau, concourant ou non à l'objet cible [3]. Cette problématique soulève plusieurs questions pour la criminalistique moderne sur le partage et le recoupement des informations afin de reconstituer la chronologie des événements. Elle met à mal une approche statique et unitaire des éléments de la scène de crime, en s'inscrivant dans une approche plus globale de la chose.

3- Exploitation et analyse des données recueillies

La littérature scientifique est riche de nombreux travaux dans l'étude des solutions connectées et de leurs artefacts, que ce soit au travers des montres, des bracelets connectés [4], des assistants vocaux [5] et plus globalement de tout dispositif connecté de la vie quotidienne [6]. Cependant, les traces obtenues résident en de nombreux fragments contenus dans une pluralité de supports d'un même réseau, susceptibles d'évoluer à travers le temps et l'espace. Afin qu'elle ne soit pas parcellaire, l'analyse ne doit pas se focaliser sur l'étude d'un unique objet mais sur l'infrastructure connectée dans son intégralité. Elle consiste donc à étudier la donnée selon trois axes : **le temps** en définissant la chronologie des évènements et des phénomènes itératifs, **l'espace** en positionnant la donnée dans l'infrastructure et au regard de l'environnement local et **le contexte** de l'évènement au regard des rôles et des actions des équipements face au phénomène. Par cette approche ternaire, l'enquêteur cherche à déterminer le cycle de vie de la donnée retrouvée, afin de la qualifier, et établir sa cohérence. Dans le but de procéder à une analyse pertinente des événements, il est nécessaire d'étudier l'information au regard d'un horodatage commun, défini à partir des caractéristiques techniques des appareils étudiés.

Par exemple, en étudiant les journaux d'évènements contenus dans la passerelle et l'application *Philips*, l'événement «lampe allumée» est horodaté. Cependant, il doit être caractérisé plus précisément. S'agit-il d'une action de l'utilisateur par le biais de l'application téléphonique, d'un interrupteur

externe, du signal d'un capteur ou d'une commande vocale au travers de l'*Amazon Echo* ? A-t-elle été effectuée par un utilisateur connu ? S'agit-il d'une action programmée ? Pour chaque question, une donnée unique est associée. Cette approche analytique est généralisable à tous les objets de l'infrastructure connectée. Ces informations déterminent les acteurs étant intervenus sur et dans l'événement, leurs positions en fonction des objets, les actions effectuées ou détectées et la réponse des objets aux différentes sollicitations.

Ainsi, les équipements regroupent des données de contexte (une configuration physique et logique d'un lieu, une habitude de vie, un enregistrement sonore ou vidéo, *etc.*) et des données à caractère personnel (une identité du consommateur de service, des informations numériques et de biométrie, *etc.*). Ces informations offrent aux enquêteurs la possibilité de reconstituer la succession des évènements avant et après l'incident. Ainsi, à partir des premiers éléments numériques, l'enquêteur est en mesure de dater l'intrusion dans le domicile de la victime avec le capteur de la porte d'entrée, le parcours du mis en cause avec le système domotique *Orvibo* corroboré par le mouvement du *Sen.se Cookie* (9), ainsi que l'heure du décès de la victime. Il peut constater l'absence de modification de la scène de crime comme un déplacement du corps de la victime post-mortem, émettre des hypothèses sur le lieu du meurtre et les circonstances. Ces informations doivent être mises en perspective avec les données médico-légales recueillies sur la scène de crime et sur la victime. Par ailleurs, les données numériques sont en mesure d'orienter certaines investigations comme des relevés de traces biologiques sur la scène de crime en fonction du parcours criminel du mis en cause. Sur une habitation de plus grande taille, ces informations aident à délimiter et à discriminer une zone d'étude en définissant une stratégie d'investigation en cohérence avec les données relevées. Les objets connectés donnent la possibilité de vérifier des hypothèses de travail en apportant de nouveaux éléments matériels, comme par exemple un mobile incohérent avec un mode opératoire. L'étude de la chronologie des évènements peut également renseigner sur une éventuelle préméditation dans la logique criminelle.

Date	Description	Source locale	Faits
T0	Lampes Philips Hue éteintes (6 et 7) Porte et fenêtre fermées (1 et 2) Etat repos : activité cardiaque de l'Apple Watch (18) et Terraillon Dot (20)	Hub Philips Hue, Hub Orvibo, iPhone (Backup Apple Watch et applications domotiques) et Terraillon Dot	Présence d'une personne en pièce 2 (connue) et aucun mouvement détecté.
10/04/2020 06:43:17	Ouverture de porte détectée (1)	Hub Orvibo et iPhone (Application domotique)	Présence d'une personne en pièce 2 (connue) et d'une personne en pièce 1 (non reconnue). Mouvements en pièce 1.
10/04/2020 06:44:03	Détection du mouvement (3)		
10/04/2020 06:44:12	Lancement de la Camera Orvibo (4)	Camera Orvibo (carte SD), Hub Philips Hue et iPhone (Application domotique)	
10/04/2020 06:52:46	Déplacement Sen.se Cookie (9)	Sen.se Mother et iPhone (Application Sen.se)	Présence d'une personne en pièce 2 (connue) et d'une personne en pièce 3 (non reconnue). Mouvements en pièce 3.
10/04/2020 06:54:16	Déclenchement IP Camera M136W	iPhone (Application IP Camera)	
10/04/2020 06:57:11	Mesure d'un mouvement Terraillon Dot (20)	Terraillon Dot	
10/04/2020 07:01:04	Mesure d'une accélération du rythme cardiaque Apple Watch (18)	iPhone (Backup Apple Watch)	
10/04/2020 07:03:39	Allumage de la Philips Hue (6) déclenchement à partir du téléphone portable iPhone SE	Hub Philips Hue et iPhone (Application domotique)	
10/04/2020 07:07:01	Mesure de l'arrêt cardiaque (8)	iPhone (Backup Apple Watch)	Présence d'une personne en pièce 2
10/04/2020 07:07:54	Fin de la mesure du mouvement Terraillon Dot (20)	Terraillon Dot	(connue).
10/04/2020 07:11:44	Détection du mouvement (3)	Hub Orvibo et iPhone (Application domotique)	Présence d'une personne en pièce 2 (connue) et d'une personne en pièce 3 puis 1 (non reconnue). Mouvements en pièce 3 et 1.
10/04/2020 08:17:21	Détection du mouvement (3) : arrivée de la patrouille		Mouvements détectés en pièce 1 et 3.
10/04/2020 08:24:56	Détection du mouvement (3)		
10/04/2020 09:12:00	Détection du mouvement (3) : arrivée enquêteur en nouvelles technologies		
T1	Lampes Philips Hue allumée (6) éteinte (7) Porte ouverte (1) et fenêtre fermée (2)	Hub Philips Hue, Hub Orvibo et iPhone (Backup Apple Watch et applications domotiques)	

4- En Bref...

L'Internet des objets contribue à l'apport subséquent d'éléments de preuves confortant un procès au pénal. Il s'avère, dans certains cas, que cette structuration étendue de l'environnement connecté peut présenter des difficultés en termes de réponse criminalistique. Les traces sont dispersées localement ou également au travers des ramifications de l'infrastructure et des espaces de traitement en ligne. Ainsi, la donnée est susceptible d'être partielle dans l'objet connecté mais devient un ensemble cohérent dans l'arborescence numérique. Cette détermination de la présence et du positionnement de l'information demeure unique à chaque écosystème. Elle est en particulier liée à la politique de la gestion de la donnée, tant au niveau du stockage que de sa synchronisation au travers du réseau. L'analyse des traces est donc beaucoup plus complexe que dans le cadre de la criminalistique numérique traditionnelle, en raison de son caractère multidimensionnel et pluridisciplinaire. Elle s'accompagne également d'un travail de contextualisation de la donnée et de compréhension de sa diffusion, selon les facteurs espace et temps. Identifier et comprendre les sources précieuses de traces est donc un défi majeur. L'ensemble de l'enquête dépend de la nature de l'appareil connecté et de l'intelligence mise en place pour sa gestion.

Références bibliographiques :

[1] Bouchaud, F., Vantroys, T., Grimaud, G.: Evidence gathering in IoT criminal investigation. In: 11th EAI International Conference on Digital Forensics and Cyber Crime. Springer (Oct 2020).
[2] Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P.: Internet of things forensics: Challenges and approaches. In: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. IEEE (Oct 2013).
[3] Attwood, A., Merabti, M., Fergus, P., Abuelmaatti, O.: SCCIR: Smart cities critical infrastructure response framework. In 2011 Developments in E-systems Engineering. IEEE (Dec 2011).
[4] Baggili, I., Oduro, J., Anthony, K., Breitinger, F., McGee, G.: Watch what you wear: preliminary forensic analysis of smart watches. In 2015 10th International Conference on Availability, Reliability and Security. IEEE (2015, August).
[5] Chung H, Park J, Lee S.: Digital forensic approaches for Amazon Alexa ecosystem. Digital Investigation (Aug 2017).
[6] Bharadwaj, N. K., Singh, U.: Acquisition and analysis of forensic artifacts from Raspberry Pi an Internet of Things prototype platform. In Recent Findings in Intelligent Computing Techniques. Springer (Nov 2019).

L'AUTEUR

Officier de la Gendarmerie nationale, le Capitaine François Bouchaud dirige le département coordination du Centre de lutte contre les criminalités numériques (C3N). Doctorant en informatique à l'Institut de recherche sur les composants logiciels et matériels pour l'informatique et la communication avancée, il est diplômé de l'École supérieure d'électronique de l'Ouest et de l'École centrale Paris.