Anàlisi de seguretat de dispositius portables connectats en xarxa sense fils Bluetooth

Josep Lluís Artacho Gallego

Grau d'Informàtica
Àrea de treball final
Seguretat informàtica

Tutor/a de TF
Gerard Farràs Ballabriga
Professor/a responsable de l'assignatura
Helena Rifà Pous

Data Lliurament 01/2023

Universitat Oberta de Catalunya

B) GNU Free Documentation License (GNU FDL)

FITXA DEL TREBALL FINAL

Títol del treball:Anàlisi de seguretat en dispositius portables connectats en xarxa sense fils Bluetooth	Anàlisi de seguretat de dispositius portables connectats en xarxa sense fils Bluetooth
Nom de l'autor:	*Josep Lluís Artacho Gallego*
Nom del consultor/a:	*Gerard Farràs Ballabriga*
Nom del PRA:	*Helena Rifà Pous*
Data de lliurament (mm/aaaa):	*01/2023*
Titulació o programa:	*Grau d'Enginyeria Informàtica*
Àrea del Treball Final:	*Seguretat informàtica*
Idioma del treball:	*Català*
Paraules clau	*Ciberseguretat , Bluetooth, IoT, privacitat comunicacions, auditoria informàtica*

Resum del Treball

Els avenços tecnològics han possibilitat la creació de nous sensors que permeten monitorar fàcilment la salut, sense ser gens invasius. Integrats dins de rellotges ''intel·ligents'', bandes d'activitat o altres dispositius portables, s'ha popularitzat dins del públic en general. Tot això, dins del marc d'una societat i dispositius hiperconnectats.

Davant el creixement de la demanda d'aquests dispositius intel·ligents amb aquestes capacitats, sorgeix el dubte sobre la seguretat que ofereixen aquest sistemes que gestionen les dades biomètriques de cada persona.

Habitualment aquest dispositius, per limitacions d'espai d'emmagatzemament, sincronitzen les dades obtingudes amb altres dispositius amfitrió (telèfon mòbil, ordinador) amb major capacitat. Aquesta sincronització es porta a terme habitualment establint una connexió sense fils mitjançant tecnologia Bluetooth entre tots dos dispositius. Precisament es aquest punt que es vol estudiar, ja que aquesta connexió té menor nivell de protecció – i per tant, més vulnerable a ciberatacs- envers altres tecnologies sense fils.

Aquest treball té com a finalitat plantejar una auditoria de seguretat -hacking ètic-, per a verificar la seguretat d'aquest dispositius o comprovar potencials riscos, estudiant la part teòrica de la tecnologia. Per a la part pràctica, amb l'ús d'eines de seguretat orientades a testejar aquest protocol. El resultat d'aquestes proves servirà per a generar un informe destinat a la millora de la seguretat.

Abstract

Technological advances have made it possible to create new sensors that allow easy health monitoring, without being invasive at all. Integrated into "smart" watches, activity bands or other wearable devices, it has become popular among the general public. All this, within the framework of a hyper connected society and devices.

Faced with the growth in demand for these smart devices with these capabilities, doubts arise about the security offered by these systems that manage each person's biometric data.

Usually these devices, due to storage space limitations, synchronize the data obtained with other host devices (mobile phone, computer) with greater capacity. This synchronization is usually carried out by establishing a wireless connection using Bluetooth technology between both devices. It’s precisely this point that we want to study, since this connection has a lower level of protection - and therefore more vulnerable to cyberattacks -,compared to other wireless technologies.

The purpose of this work is to propose a security audit – ethical hacking -,to verify the security of these devices or check potential risks, studying the theoretical part of the technology. For the practical part, with the use of security tools aimed at testing this protocol.

The result of these tests will be used to generate a report aimed at improving safety.

Índex

Llista de figures

Annex

1. Introducció

Els avenços tecnològics han possibilitat la creació de nous dispositius i sensors que permeten monitorar fàcilment la nostra salut, integrats a rellotges ‘’intel·ligents’’, bandes d’activitat o altres dispositius a l’abast del públic en general, més enllà del públic especialitzat (sistemes mèdics, esportistes d’alta competició, atletes). Fins i tot, poden donar consells d'entrenament en funció de l’activitat física que pugui detectar mitjançant la xarxa de sensors que incorporen per a captar diferents dades biomètriques de la persona o de la ubicació on es trobi l’usuari. En alguns dispositius de gamma alta poden arribar a emetre un avís d’emergència en cas que l’usuari pugui patir una caiguda o pèrdua de consciència.[1]

Habitualment aquest dispositius, per limitacions d’espai de emmagatzemament i de memòria, sincronitzen les dades obtingudes amb altres dispositius amfitrió (telèfon mòbil, ordinador) amb major capacitat. Aquesta sincronització es porta a terme habitualment establint una connexió sense fils mitjançant tecnologia Bluetooth entre tots dos dispositius.

Davant el creixement de la demanda[2] [3]d’aquests dispositius intel·ligents amb aquestes capacitats, sorgeix el dubte sobre la seguretat que ofereixen aquest sistemes que gestionen les nostres dades biomètriques: pes, ritme cardíac, temperatura corporal, nivell d'oxigen a la sang, hores d’activitat, son, cicle menstrual i fins i tot, dades d’embaràs.[4]

1.1. Context i justificació del Treball

Aquest treballs té com a objectiu fer un estudi de la seguretat integrada als dispositius IoT (Internet of Things), en particular rellotges intel·ligents, monitors d’activitats o similars. Concretament, es vol comprovar el comportament d’aquest sistemes davant intents de connexió o anàlisi fent servir la connexió sense fils Bluetooth, mitjançant eines d’auditoria (hacking ètic).

La idea és explorar possibles riscos de seguretat en fer servir aquest tipus de connexió, especialment si està activa i sense vincular a cap dispositiu. Es molt freqüent que per desconeixement dels usuaris, aquesta connexió quedi oberta i detectable per altres dispositius. En cap cas es pretén accedir al contingut del dispositiu, per tal de respectar la privacitat dels usuaris.

1 https://www.aarp.org/espanol/hogar-familia/tecnologia/info-2020/relojes-inteligentes-monitoreo-alertas-emergencia-para-cuidadores.html
2 https://www.itreseller.es/en-cifras/2022/09/las-ventas-de-wearables-alcanzaran-los-344-millones-de-unidades-a-finales-de-2022
3 https://www.itreseller.es/en-cifras/2022/02/el-mercado-mundial-de-wearables-crecera-un-132-en-2022
4 https://topesdegama.com/listas/wearables/smartwatches-salud

1.2. Objectius del Treball

Els objectius que es pretén aconseguir amb aquest projecte son:

- Estudi de la tecnologia sense fils Bluetooth. Estat de l'art.
- Estudi de les picoxarxes, xarxes per intercanvi de dades als dispositius IoT.
- Ús d'eines per comprovar la seguretat de la xarxa.
- Preparació de l'entorn de proves amb les eines d'auditoria.
- Verificació de la seguretat dels dispositius davant riscos.
- Proposar mesures per reduir aquest riscos.
- Marc legal.

1.3. Impacte en sostenibilitat, ètic-social i de diversitat

Sostenibilitat
Aquest treball tracta de la seguretat dels dispositius i de les comunicacions entre ells. De fer un bon ús.

Per a la realització de la part pràctica, es faran servir equips virtuals per reaprofitar recursos.

Compromís ètic
En tot moment, aquest treball té present les consideracions ètiques i legals que implica analitzar un sistema de forma honesta, per a cercar possibles errades de seguretat o configuracions incorrectes que puguin permetre accedir de formar irregular o simular errors.

Impacte positiu / negatiu
En un principi, aquest treball es va dissenyar tenint present un impacte negatiu referent a la poca seguretat que ofereix la interconnexió dels dispositius.

Per altre banda, l'objectiu final es la millora de la seguretat, mitigar errades de seguretat i fer una guia de bones pràctiques per tal de salvaguardar les dades personals i biomètriques contingudes al dispositiu. Per tant, podem tenir un impacte positiu en quant al tractament i seguretat de dades.

Diversitat
En aquest treball s'escriu i tracta de les dades de les persones que poden recopilar els dispositius sense fer distincions de gènere, raça, religió, orientació sexual o ideologia.

1.4. Enfocament i mètode seguit

L'enfocament d'aquest treball es fer un estudi de la comunicació entre els dispositius, per a posteriorment poder avaluar la seguretat d'un sistema mitjançant eines d'anàlisi, inspecció de paquets i amb un dispositiu a mode d'amplificador de senyal Bluetooth.

Per aquesta tasca, es farà servir la distribució Linux Kali que integra diverses eines per tal efecte. Aquesta distribució es una derivació actualitzada de la distribució BackTrace utilitzada a la assignatura Seguretat de Xarxes de Computadors. Per aquesta tasca, es valorarà l'ús d'una maquina virtual preconfigurada amb el sistema de virtualització Oracle VirtualBox.

Es farà una prova de camp per determinar quins dispositius son detectables dins d'un àrea. Es a dir, es realitzarà proves d'anàlisi dins d'un entorn controlat amb un dispositiu i en altre, obert. Aquest últim, amb l'objectiu de comprovar quins dispositius en una àrea determinada es troben en mode «detectable», susceptibles de poder ser analitzats.

Per motius ètics i legals, per fer aquesta prova es comptarà amb usuaris voluntaris que vulguin posar a prova el seu dispositiu. L'objectiu es que el dispositiu a analitzar pugui establir comunicació amb l'equip auditor i en cap cas – a diferencia d'un cas real de ciberatac-, accedir a dades del dispositiu.

Amb aquest recull de dades, podem determinar el tipus de dispositiu i les seves possibles vulnerabilitats (exploits), si n'hi ha reportades. També, podem comprovar si el fabricant ha publicat alguna actualització del sistema per tal d'evitar aquest problemes.

1.5. Planificació del Treball

La planificació temporal prevista té com a base el calendari de lliuraments del pla docent de l'assignatura. Amb aquestes dades i fites, es genera un diagrama de Gantt amb l'aplicació ProjectLibre:

	Nombre	Duracion	Inicio	Terminado	Predecesores
1	PAC 1 - Proposta de treball	8 days?	30/09/22 8:00	11/10/22 17:00	
2	Definició objectius	2 days?	30/09/22 8:00	3/10/22 17:00	
3	Recerca fonts	5 days?	3/10/22 8:00	7/10/22 17:00	
4	Redacció PAC	2 days?	8/10/22 8:00	11/10/22 17:00	
5	PAC 2 - Seguiment del projecte. Lliurament parcial	20 days?	12/10/22 8:00	8/11/22 17:00	1
6	Estudi sistemes sense fils	5 days?	12/10/22 8:00	18/10/22 17:00	
7	Instalació aplicatius analisi	2 days?	19/10/22 8:00	20/10/22 17:00	
8	Testeig sistema auditor	2 days?	21/10/22 8:00	24/10/22 17:00	
9	Proves análisi dispositiu control	3 days?	25/10/22 8:00	27/10/22 17:00	
10	Analisi dispositiu - auditoria	3 days?	28/10/22 8:00	1/11/22 17:00	
11	Redacció PAC	6 days?	1/11/22 8:00	8/11/22 17:00	
12	PAC 3 - Seguiment del projecte	20 days?	9/11/22 8:00	6/12/22 17:00	5
13	Ampliació análisi auditoria	7 days?	9/11/22 8:00	17/11/22 17:00	
14	Processat de les dades obtingudes	6 days?	18/11/22 8:00	25/11/22 17:00	
15	Redacció PAC	6 days?	28/11/22 8:00	5/12/22 17:00	
16	PAC 4 - Lliurament definitiu. Memòria final	25 days?	7/12/22 8:00	10/01/23 17:00	12
17	Analisi resultats	10 days?	7/12/22 9:00	21/12/22 9:00	
18	Conclusions	5 days?	17/12/22 9:00	23/12/22 17:00	
19	Redacció PAC	9 days?	26/12/22 8:00	5/01/23 17:00	
20	Revissió documentació total a lliurar	2 days?	8/01/23 9:00	10/01/23 17:00	
21	PAC 5 - Presentació en vídeo	5 days?	11/01/23 8:00	17/01/23 17:00	16
22	Preparació presentació	3 days?	11/01/23 8:00	13/01/23 17:00	
23	Preparació video	2 days?	14/01/23 9:00	17/01/23 17:00	
24	PAC 6 - Defensa asíncrona del projecte	5 days?	23/01/23 8:00	27/01/23 17:00	21

Figura 1: Planificació treball. Calendari.

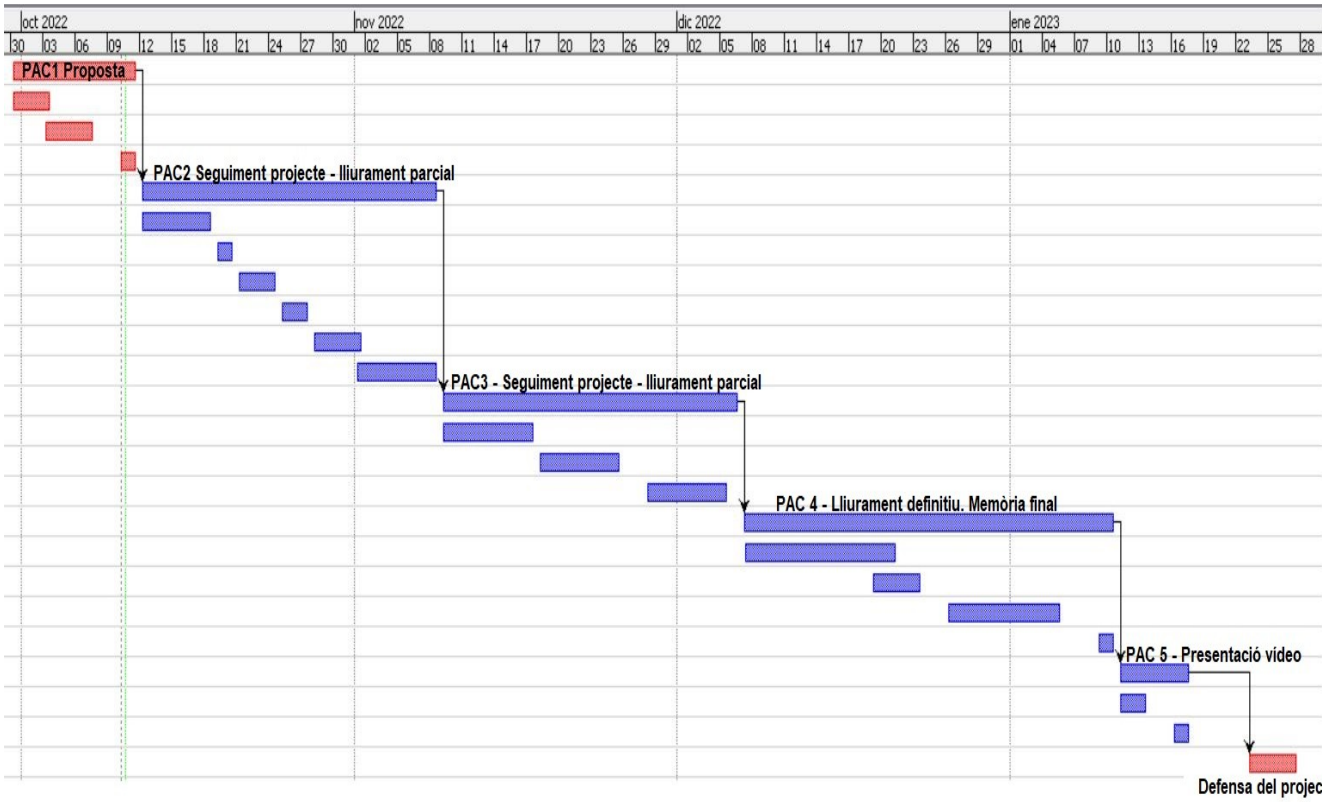

Figura 2: Planificació treball. Diagrama de Gantt

1.6. Breu sumari de productes obtinguts

El producte final serà un document a mode d'informe auditor on s'indicaran:

- Dispositius que s'han detectat i analitzat, anonimitzant dades que puguin identificar a l'usuari.
- Tècnica emprada per fer l'anàlisi.
- Risc detectat.

1.7. Breu descripció dels altres capítols de la memòria

Capítol 1. Proposta de treball i planificació temporal. Introducció i objectius.

Capítol 2. Material i mètodes. Estudi de les tecnologies emprades als dispositius i de les eines auditores.

Capítol 3. Resultats. Execució de les proves de seguretat als dispositius.

Capítol 4. Conclusions i treballs futurs. Reculls de les dades obtingudes i generació de l'informe d'auditoria.

Glossari.

Bibliografia.

Annexos. Informació de les eines usades al projecte.

2. Materials i mètodes

2.1. Introducció. Connectivitat dispositius Bluetooth

Els dispositius que son objecte d'estudi, tenen la capacitat de connexió mitjançant la tecnologia sense fils Bluetooth.

Aquesta tecnologia permet interconnectar fàcilment dispositius a mode de petites xarxes sense fils personals (PAN) per transmetre veu i dades entre dispositius que estiguin físicament a prop, dins d'un rang de 10 metres. En funció de la versió, la velocitat de transmissió és de 720 kb/s fins a 50Mb/s i cobrir distancies fins a 120 metres amb l'ús de repetidors.

Les normes, desenvolupament i especificacions de Bluetooth es gestionen mitjançant l'associació sense ànim de lucre (*Bluetooth Special Interest Group, Inc - SIG*)[5] [1].

Aquest grup, es va constituir al 1998 per les companyies Ericsson, Nokia i Intel, a les que també es van afegir IBM i Toshiba, amb l'objectiu de col·laborar per a estandarditzar la connectivitat de curt abast entre diferents dispositius i industries. Mes endavant, (1999) es van unir com a promotors 3Com, Lucent, Motorola i Microsoft.

Actualment (octubre 2022), en formen part de SIG més de 36000 socis, que inclouen a la majoria de fabricants de dispositius, companyies de telecomunicacions, informàtica i d'altres sectors industrials i audiovisuals.

El nom i el logotip, té com origen la historia antiga escandinava. Es tracta d'un curiós homenatge al rei danès i noruec Harald Blåtand que va unir els pobles danès i noruec al 958. Aquest fet, tenia cert paral·lelisme amb l'idea original del SIG de poder unir PC i la telefonia mòbil, amb un enllaç sense fils.
Aquest personatge històric, atès que tenia una dent fosca (o blava, en nòrdic antic), va rebre el sobrenom de «dent blava» (*bluetooth* en anglès). El logotip es la fusió dels caràcters rúnics Futhark el jove Hagall (ᚼ) i Bjarkan (ᛒ) que representen les inicials del seu nom, H i B

Logotip de Bluetooth. (c) Propietat i marca registrada del Bluetooth SIG i afiliats (https://www.bluetooth.com/terms-of-use/)

5 Dades i web oficial del SIG: https://www.bluetooth.com/

2.2. Conceptes funcionament Bluetooth

La tecnologia Bluetooth es defineix com una especificació industrial que possibilita la transmissió de veu i dades entre diferents dispositius emparellats per radiofreqüència a la banda ISM[6] de 2,4Ghz. (2,402-2,480 GHz).
Aquesta especificació correspon a la IEEE 802.15.1 [7]

L'abast de radio dels dispositius Bluetooth depèn de la potència de transmissió. En funció d'aquesta potència, es classifiquen en tres classes:

- Classe 1: 100 mW, amb un abast de 100 metres.
- Classe 2: 2,5 mW, amb un abast de 10 metres.
- Classe 3: 1 mW, amb un abast de 1 metre.

Per que un dispositiu pugui connectar-se amb un altre, es necessari que cadascú pugui suportar unes descripcions (perfils) que defineixen el seu comportament i funcionalitats.

Actualment hi ha dos tipus d'implementació del protocol Bluetooth que es diferencien en la forma de modulació del senyal, la pila o protocol de comunicacions i el consum elèctric:

- Bluetooth Clàssic (Basic Rate / EDR): orientat per la transmissió de gran quantitat de dades. La transmissió de dades es realitza utilitzant 79 canals dins de la banda de 2,4Ghz a intervals de 1Mhz. Aquest mètode permet transmetre dades fins a 3 Mb/s

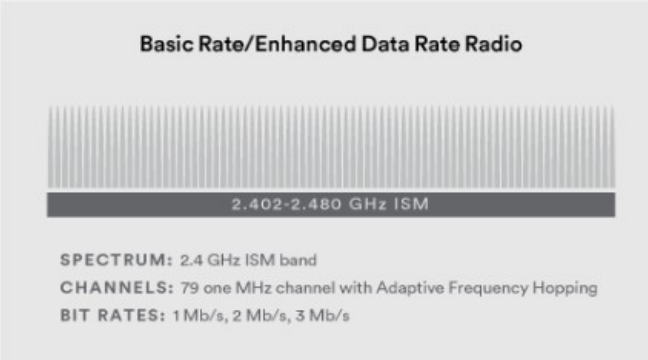

Figura 3. Transmissió dades Bluetooth Clàssic (BR /EDR)
font: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

6 La banda ISM es una part de l'espectre de radiofreqüències reservada internacionalment i oberta a tothom sense necessitat de llicència. Està destinada a usos no comercials en àmbits industrials, científics i mèdics: https://es.wikipedia.org/wiki/Banda_ISM

7 IEEE 802.15.1: https://standards.ieee.org/ieee/802.15.1/1180/

- Bluetooth Low Energy (BLE): orientat a l'intercanvi de petites quantitats de dades cada cert temps, amb un consum elèctric molt reduït. Per això, la transmissió de dades es realitza utilitzant 40 canals dins de la banda de 2,4Ghz a intervals de 2Mhz.

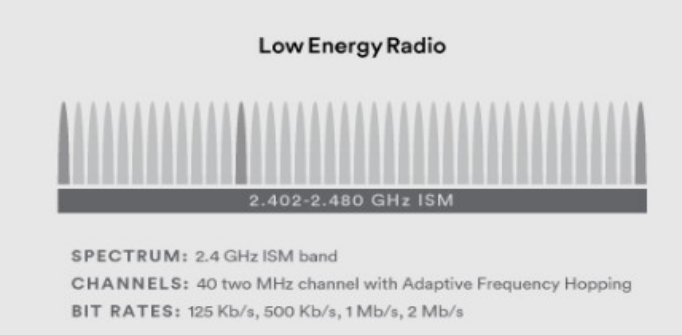

Figura 4. Transmissió dades Bluetooth BLE
font: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

2.2.1. Versions

Des de la presentació de la tecnologia fins ara, s'han realitzat cinc versions.

- Bluetooth 1.x: primera versió que es va presentar al maig de 1998, actualment gairebé ja no es fa servir. Tenia problemes de seguretat relacionats amb el emparellament de dispositius. La velocitat de connexió arribava fins a 1Mb/s.

- Bluetooth 2.x: presentada a l'any 2005, va tenir molt èxit entre els telèfons mòbils avançats degut al procès simplificat d'emparellament. Suporta velocitats de transmissió de fins a 3Mb/s.

- Bluetooth 3.x: presentada l'abril del 2009. Suporta velocitats de transmissió fins a 24Mb/s, però amb consum elèctric més elevats que les generacions anteriors.

- Bluetooth 4.x: presentada al juny de 2010. La principal novetat es la implementació de l'especificació de Bluetooth de molt baix consum elèctric (Bluetooth Low Energy – BLE). Aquest fet va permetre integrar aquesta connectivitat als dispositius IoT (Internet de les coses - idC)[8], alimentats per petites piles / bateries.

  Altres millores en aquesta versió: alta velocitat (25-32 Mb/s) i gran abast de connexió (50 a 100 metres).

8 Iot: acrònim anglès Internet of Things. En català IdC: Internet de les coses.
Font: www.termcat.cat

Mes endavant, amb la presentació de la versió BLE 4.2, es va afegir el protocol IPv6 a la pila de BLE. Això ha possibilitat que dispositius IoT/idC utilitzant el protocol BLE, tinguin comunicació Internet via IPv6

- Bluetooth 5.x: presentada a l'any 2016. Suporta velocitats de transmissió fins a 50 Mb/s, rang de cobertura estable de 120 metres. Manté el baix consum elèctric presentat a la versió 4.x.
  La darrera versió presentada (Bluetooth 5.2), implementa funcions de posicionament. Això permet a un dispositiu determinar la presència i geolocalització d'altre dispositiu en interiors.

A la taula de la figura 5, podem veure els diferents entorns d'ús dels dos tipus de versions.

Application scenario	**Audio stream application** Wireless head-phones Wireless speaker Vehicle-mounted entertainment	**Data transmission application** Sports and fitness equipment Medical and health equipment Peripherals and accessories	**Location services application** Beacon services Indoor navigation service Asset tracking	**Device network application** Control system Monitoring system Automation system
Communication mode	One-to-one	One-to-one	One-to-many (broadcast)	Many-to-many (mesh)
Radio frequency mode	Classic Bluetooth BR/EDR	Bluetooth low energy (Bluetooth LE)		

Figura 5. Comparativa Bluetooth Clàssic vs BLE
font: https://blog.nordicsemi.com/getconnected/the-difference-between-classic-bluetooth-and-bluetooth-low-energy

Aquestes diferencies fa que dispositius amb diferents versions de protocol no pugin comunicar-se entre ells.

Per altra banda, les versions Bluetooth son retrocompatibles. Si més no, els dispositius poden implementar dos modes de funcionament per poder interactuar amb altres versions:

- Single mode: només funciona amb versió BLE
- Dual mode: suporta les dues implementacions, BLE i Clàssic.

La taula de la figura 6, mostra les diferencies de la pila de comunicacions de totes dues implementacions single mode / dual mode:

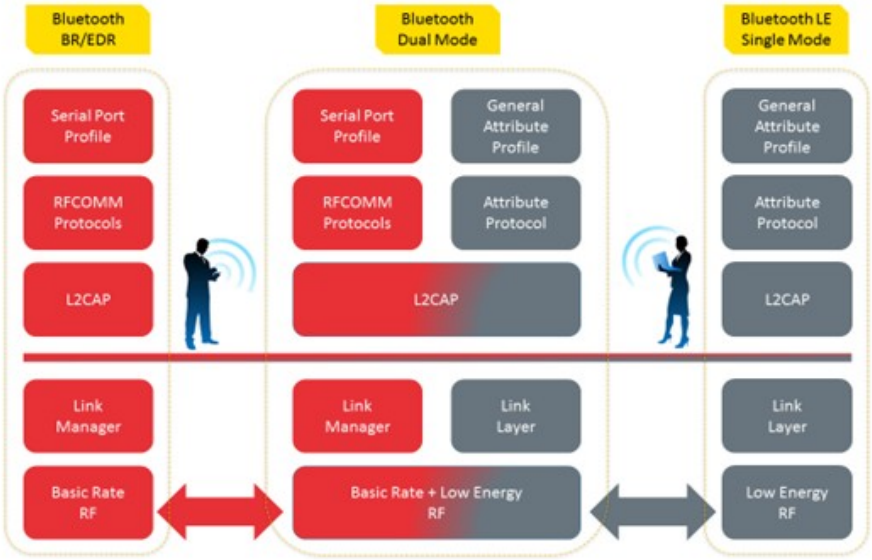

Figura 6. Comparativa estructura de pila de comunicacions single/dual mode
Font i origen imatge: https://www.incibe-cert.es/blog/analizando-bluetooth

2.3. Procés de connexió dels dispositius

Per poder encriptar la connexió entre els dos dispositius, s'ha de establir una connexió SSL entre ells. Consta de dues parts:

- Dispositiu esclau: envia paquets periòdicament, quedant a l'espera de resposta del dispositiu màster,
- Dispositiu màster: verifica les peticions de connexió i inicia el procès de connexió.

Un esdeveniment de connexió succeeix quan dos dispositius intercanvien informació periòdicament després d'establir connexió. En el cas de BLE, els dispositius poden estar en mode repòs i activar-se només en cas d'un esdeveniment de connexió, intercanviar dades i tornar al mode repòs.

Tot i que BLE fa servir criptografia AES-CCM, els mecanismes d'intercanvi de claus de Bluetooth tenen algunes vulnerabilitats que poden permetre a un atacant comprometre aquesta seguretat.

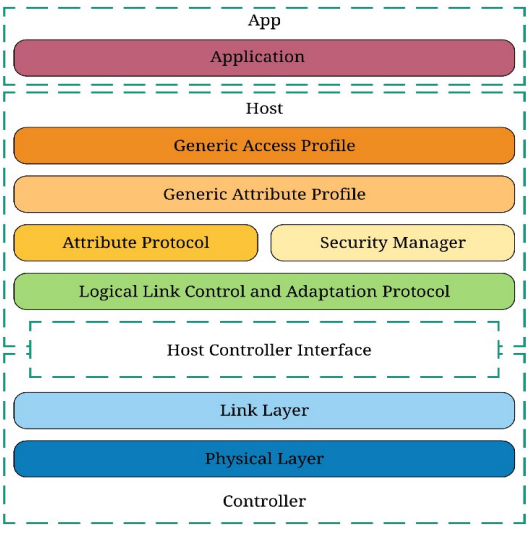

Figura 7. Pila comunicacions BLE

Font i origen imatge: [2] BARUA et al.: SECURITY AND PRIVACY THREATS FOR BLUETOOTH LOW ENERGY IN IoT AND WEARABLE DEVICES. Volume 3 2022, pg 255

El paràgraf següent i la figura 8, mostra el procès d'intercanvi de claus i els possibles riscos de seguretat. Aquest procès es gestionat pel gestor de seguretat (Security Manager). Consta de tres fases:

- Fase I: s'inicia en el moment que un dispositiu envia una petició de emparellament (pairing request) cap altre. En aquest moment, hi ha un intercanvi de dades dels dos dispositius per a especificar el tipus, autenticació, mida de l'enllaç i poder triar el mètode d'emparellament adient. Aquestes dades intercanviades s'envien en text pla, amb el risc que puguin ser interceptades per un atacant.

- Fase II: s'inicia en finalitzar la fase anterior.
Seguint un model de clau publica / privada, es generen les claus TK partint d'un valor aleatori de 128 bits (Srand / Mrand) que genera cada dispositiu. Aquestes claus permeten generar la clau STK per encriptar la comunicació entre els dos dispositius. El punt feble que hi ha es que les dades (Srand / Mrand) s'intercanvien en text pla. Un possible atacant, amb les claus Srand / Mrand capturades, podria arribar a calcular la clau STK

- Fase III: en aquest fase de vinculació, se intercanvien claus específiques de transport encriptat STK. La major part de les claus es generen pel dispositiu esclau.

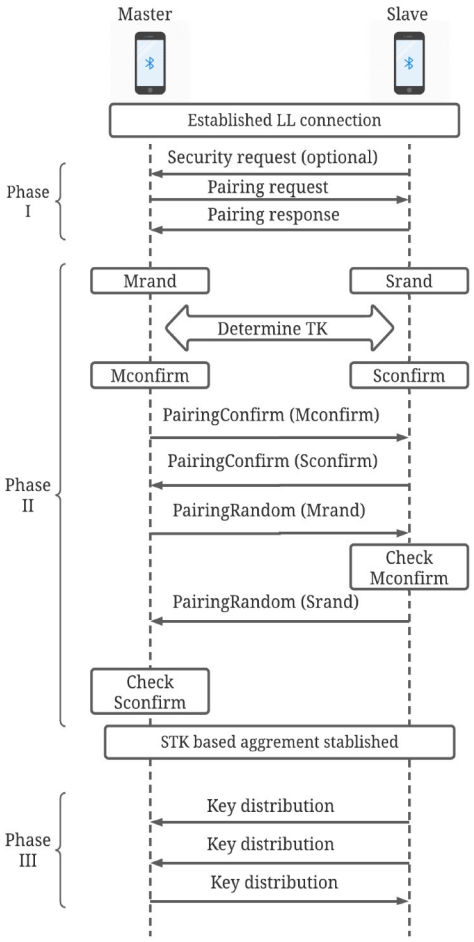

Figura 8. Fases de connexió BLE

Font i origen imatge: [2] BARUA et al.: SECURITY AND PRIVACY THREATS FOR BLUETOOTH LOW ENERGY IN IoT AND WEARABLE DEVICES. Volume 3 2022, pg 257

2.4. Anàlisi de vulnerabilitats i riscos

La figura annexa, mostra els diferents tipus d'atac que pot patir un dispositiu Bluetooth.

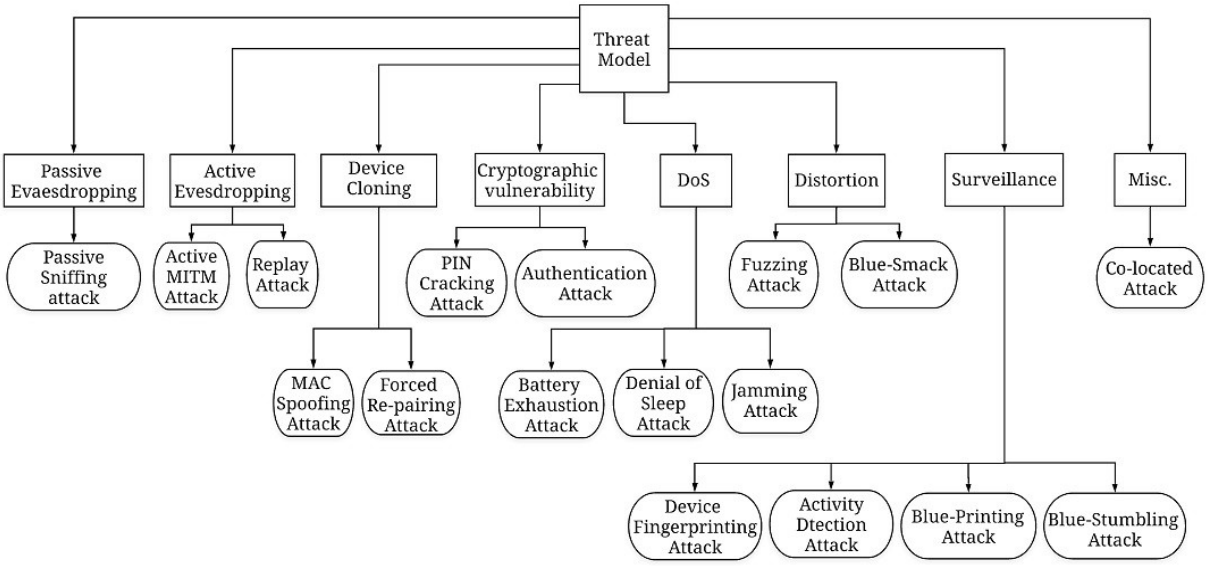

Figura 9. Estructura d'amenaces sota BLE
Font i origen imatge: [2] BARUA et al.: SECURITY AND PRIVACY THREATS FOR BLUETOOTH LOW ENERGY IN IoT AND WEARABLE DEVICES. Volume 3 2022, pg 260

Revisant aquesta taula, es pot comprovar que uns dels principals avantatges de la tecnologia Bluetooth que es la facilitat de connexió, es també el seu principal problema. Especialment, en dispositius més senzills amb poca capacitat de processament i per tant, més vulnerables a patir un atac.

Realitzant una prova real com a prova de concepte dins d'una ubicació força concorreguda (transport públic, cafeteria...) s'ha pogut detectar múltiples dispositius tipus portables (polseres d'activitats, rellotges intel·ligents, auriculars...). En aquest cas, només fent servir un telèfon mòbil (Android 10), activant la connexió Bluetooth i fer una recerca dels dispositius amb la connexió Bluetooth oberta al voltant. La figura 10, conté varies captures de pantalla mostrant els resultats, en diferents hores. La figura 11, mostra dispositius IoT: llums intel·ligents, tancaments electrònics...

Aquest tipus d'auditoria on només recopilem dades té el sobrenom de *Bluebag*[9] [3]Per contra, aquesta metodologia es la base d'un atac de recerca d'empremtes (Fingerprinting attack) on un hipotètic atacant amb eines més elaborades, podria fer servir aquesta recerca per determinar quins dispositius poden ser susceptibles de ser atacats. A la taula 8, aquest riscos es trobarien dins de la secció de vigilància (Surveillance): Fingerprinting attack, activity detection attack, blue-printing attack, Blue-Stumbling attack.

9 Experiment Bluebag: https://www.acta.es/medios/articulos/ergonomia_y_seguridad/053049.pdf, pg.53

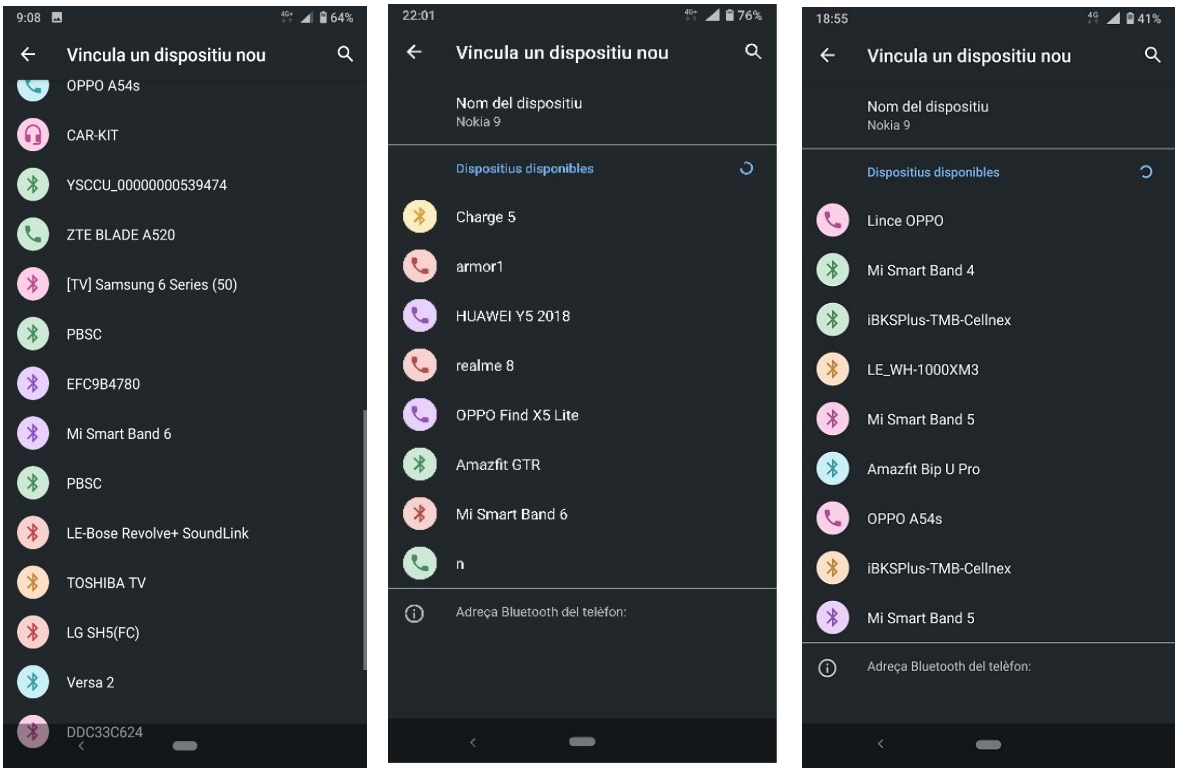

Figura 10. Rastreig dispositius
Font: elaboració pròpia

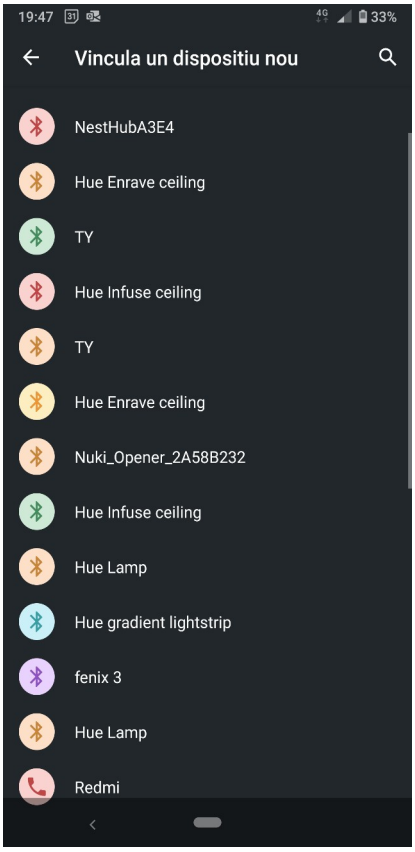

Figura 11. Rastreig dispositius Iot
Font: elaboració pròpia

2.5. Plataforma d'anàlisi: entorn auditor

Per a la realització d'aquest treball, s'ha construït una plataforma d'anàlisi que constitueix el nostre entorn auditor. Aquesta plataforma està formada per una maquina virtual on s'instal·la la distribució de seguretat Linux Kali sota l'entorn de virtualització Oracle VirtualBox, que es combina amb un dispositiu USB (Ubertooh One) amb funcions de captura i injecció de tràfic de senyal Bluetooth.[4]. Aquest dispositiu compta també amb programari de suport que complementa algunes utilitats específiques per tractar els senyals del protocol Bluetooth.

Donat que algunes proves de captures de dades requereixen mobilitat geogràfica, tot aquest sistema s'ha instal·lat amb un equip portàtil[10] amb suficients recursos de maquinari per gestionar sense problemes les proves.

Llevat del sistema operatiu de l'equip amfitrió -Microsoft Windows 10 Pro -, tot el programari utilitzat es Open Source. Fins i tot, el dispositiu Ubertooth One està també desenvolupat sota codi obert.

Les característiques dels components, consideracions de disseny, així com la instal·lació i posada en funcionament de cada component, es descriu al capítol 7 de l'annex d'aquest treball.

Figura 12. Equip com a plataforma d'anàlisi
Font: elaboració pròpia

10 Característiques principals de l'equip utilitzat : Fujitsu Lifebook U757: CPU Intel Core i7 7500, 16 Gb RAM DDR4, disc SSD 500Gb, pantalla 15,6 polsades FHD. Wlan Intel(R) Dual Band AC 8265 i Bluetooth 5.0 S.O. Windows 10 Pro 21H2. Addicionalment, la màquina virtual s'instal·la en un disc extern 500Gb SSD, connectat a l'equip per USB C (5.0 Gb/s)

3. Resultats

En aquest capítol, s'executaran les diferents proves per recollir dades i resultats de les proves de connexió de diferents dispositius, en diferents entorns. Bàsicament, es farà un exercici de captura de les trames dels dispositius (Passive sniffing attack) per tal d'identificar-los, segons la seva adreça MAC (anomenada BD-ADDR en Bluetooth). En cap cas, es recullen dades que puguin identificar a la persona propietària o bé, s'anonimitzen.

Per aquesta tasca, es faran servir les eines d'anàlisi Bluetooth més bàsiques incloses amb Kali i les Ubertools. No s'utilitzaran altres eines més agressives (Kismet, spooftooph), que poden arribar a mostrar i capturar més dades. Es vol comprovar la seguretat dels dispositius sense posar en risc la privacitat de les dades dels usuaris.

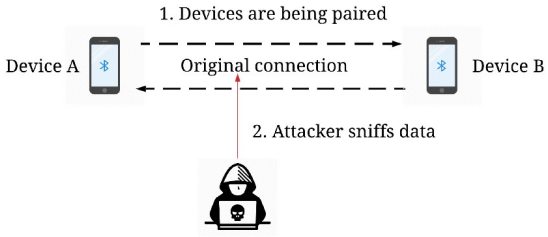

Figura 13. Exemple d'atac d'escaneig passiu (passive sniffing attack)
Font i origen imatge: [2] BARUA et al.: SECURITY AND PRIVACY THREATS FOR BLUETOOTH LOW ENERGY IN IoT AND WEARABLE DEVICES. Volume 3 2022, pg 260

Per la part de maquinari, farem les proves amb els mòduls Bluetooth de l'equip amfitrió i amb Ubertooth One. Això permet comprovar la diferencia en quant al processat entre un mòdul convencional i altre específicament dissenyat per auditar.

Totes aquestes dades, ens servirà per arribar a les conclusions que es tractaran al capítol quart.

3.1. Proves de connexió amb dispositius Bluetooth 1.1

Iniciem les proves de connexió per a la recerca de vulnerabilitats dins d'un entorn controlat. En aquest cas, es realitzen les proves amb un antic kit de GPS del fabricant PalmOne comercialitzat a l'any 2005 que sabem que no està actualitzat al tractar-se d'un sistema descatalogat i sense suport fa temps, però encara operatiu. Aquest kit serà l'equip de control per iniciar les proves prèvies a un entorn més real.

Aquest kit està compost per una PDA Palm Zire 72[11] amb sistema operatiu PalmOs 5.2.8 interconnectada per Bluetooth amb un mòdul GPS extern (Kirrio). Tots dos dispositius utilitzen la versió del protocol Bluetooth 1.1. A la fotografia de la figura 11, mostra els dispositius emparellats i en funcionament.

11 Palm Zire: https://es.wikipedia.org/wiki/Zire_72

Tots dos dispositius son propietat de l'autor d'aquest treball, per tant no hi ha risc d'incompliment legal d'accés no autoritzat.

Figura 14. Dispositius Palm Zire i mòdul GPS extern (Kirrio) Font: elaboració pròpia

La pantalla de la PDA mostra el nivell de senyal dels satèl·lits de posicionament que està detectant el mòdul GPS que li envia via connexió Bluetooth. La part de geolocalització es gestiona mitjançant l'aplicació MapSonic.

Tot i que en aquesta prova es realitza en un entorn controlat, farem una etapa inicial de reconeixent dels dispositius que hi ha al voltant. Per aquesta tasca, farem servir les eines de programari incloses a Kali.

S'executa la comanda `sudo hcitool scan` que ens mostra l'adreça dels dispositius Bluetooth BR que hi ha al voltant i que no estan emparellats:

```
File  Actions  Edit  View  Help
└─$ sudo hcitool scan
Scanning ...
        48:7E:48:C9:5D:DE       Realtek Bluetooth
        00:07:E0:40:90:C9       Zire
        00:0D:B5:01:00:28       BT-GPS-010028
```

Figura 15. Resultat comanda *sudo hcitool scan*

Podem observar que, a banda dels nostres dispositius, hi ha un tercer aliè a la prova (Realtek Bluetooth). Per tant, s'exclou aquest dispositiu de qualsevol prova.

Obtenim més informació detallada dels dispositius amb la comanda:
`sudo hcitool scan --info`

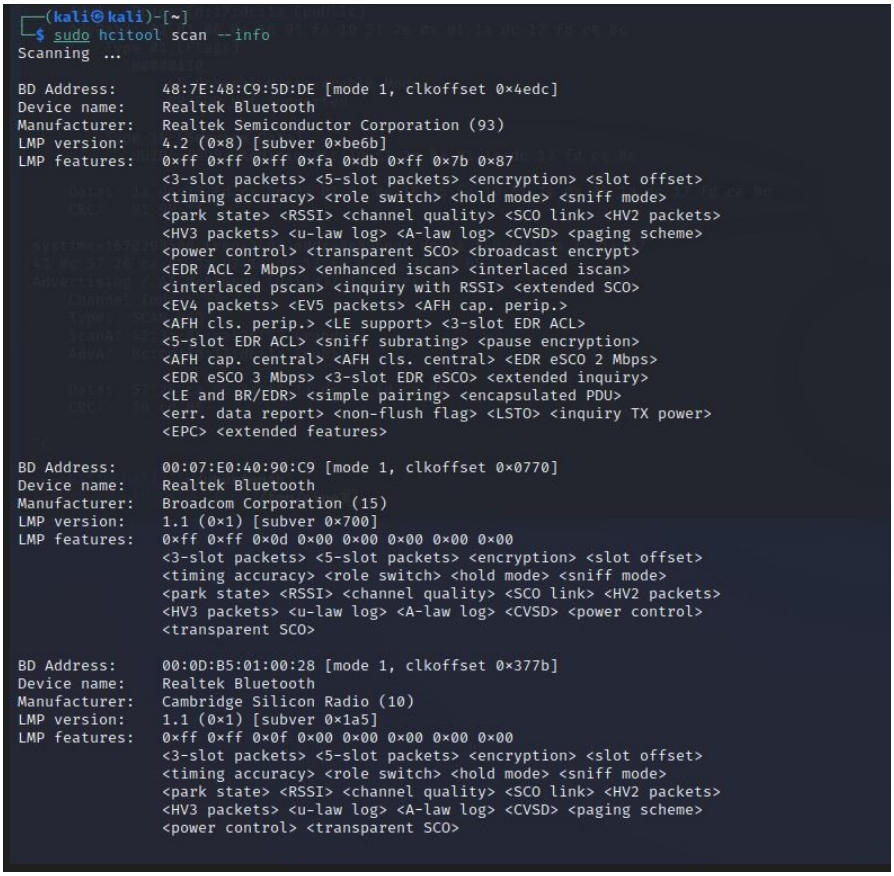

Figura 16. Resultat comanda *sudo hcitool scan --info*

En aquest cas, es mostra informació més concreta de cada dispositiu: fabricant del receptor de radiofreqüència Bluetooth (Manufacturer), versió del protocol Bluetooth implementada (LMP version) i característiques (LMP features).

Addicionalment, sabent que els tres primers dígits de la BD-ADDR identifica al fabricant, podem recopilar més informació als següents llocs web només introduint els tres primers dígits, o bé tota la MAC o BD ADDR

https://mac.lc/

https://www.wireshark.org/tools/oui-lookup.html

Amb el resultat de la comanda inicial, ja sabem exactament l'adreça de cada dispositiu i poder fer una prova de connexió. En aquest cas, farem un duplicat de la adreça MAC Bluetooth del mòdul GPS fent servir les eines de la sonda Ubertooth per simular un atac de suplantació (MiTM – Man in the Middle).

Des de un terminal, executem la comanda de ubertools per enviar paquets amb la MAC que es passa com argument amb el paràmetre -s

```
ubertooth-btle -s 00:0D:B5:01:00:28
```

Passat uns segons, podem comprovar que el dispositiu «fals» apareix al gestor de Bluetooth Kali BlueManager

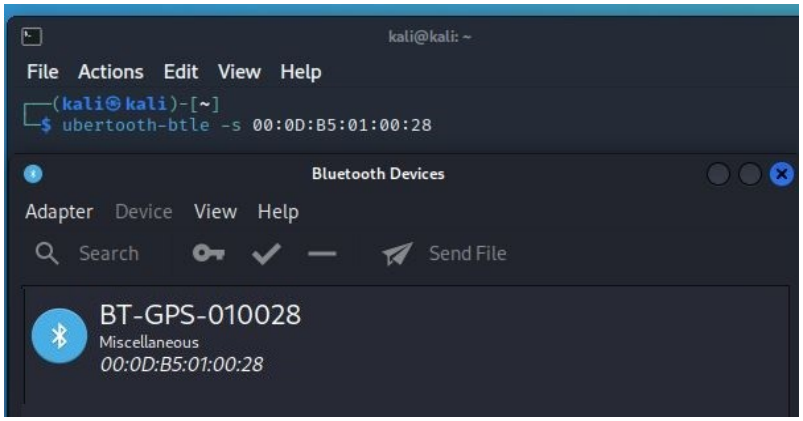

Figura 17. ***Dispositiu clonat***

Intentem emparellar el dispositiu:

Figura 18. Dispositiu clonat detectat

Si més no, la PDA s'intenta emparellar però es desconnecta als pocs segons, tornant a la pantalla de tria de dispositius. Una de les raons es que el dispositiu emulat i la PDA tenen versions diferents del protocol Bluetooth.

A Wireshark podem veure la trama:

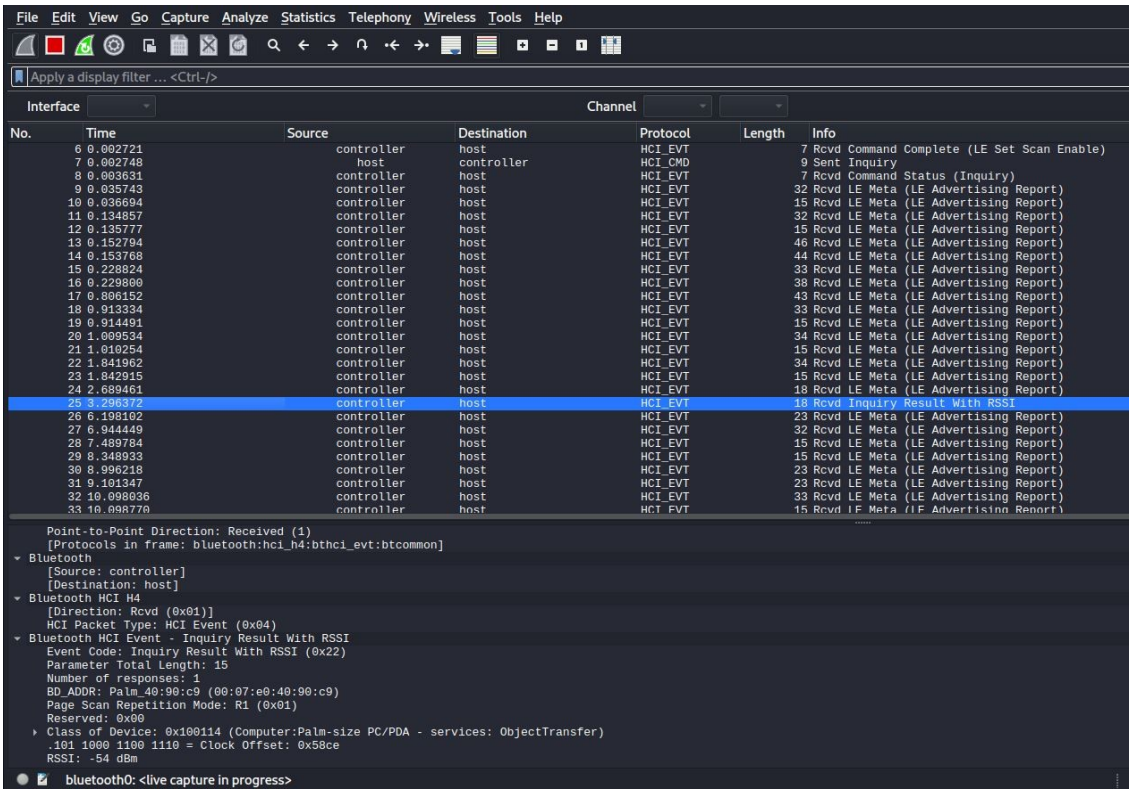

Figura 19. Trama de connexió

Finalment, en encendre el mòdul GPS autèntic es vinculen correctament. En seguir forçant la connexió cap al dispositiu fals apagant el mòdul real, es provoca que la PDA quedi bloquejada.

El resultat de la prova provoca que la PDA es quedi completament bloquejada en el moment de fer la connexió, sense resposta al botó d'encegada ni cap altra combinació de tecles. Malauradament, per treu-re la PDA d'aquest estat s'ha de reiniciar (botó reset a la part darrera de la PDA). Al fer això, el contingut emmagatzemat a la memòria (RAM i emmagatzemament) s'esborra.

La figura 20, mostra la seqüència i el resultat posterior. Per defecte, la PDA canvia el nom a «Computadora de mano Palm»

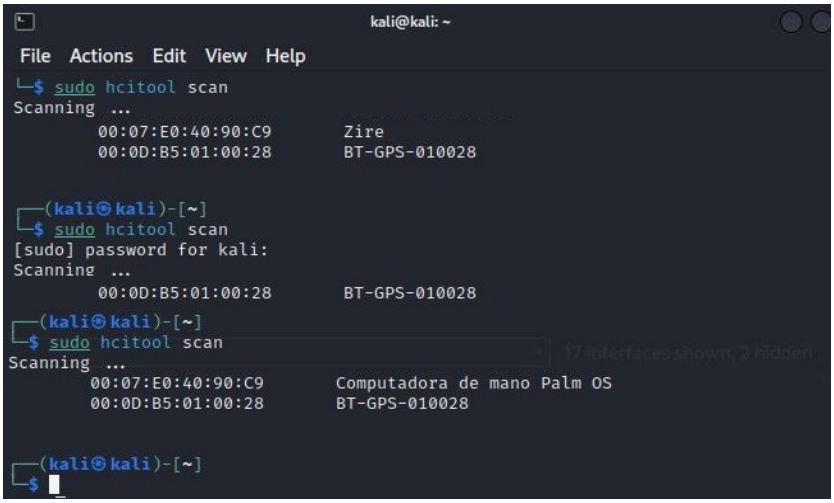

Figura 20. Seqüència atac

En aquest cas, va ser necessari restaurar una copia de seguretat al dispositiu Palm per disposar dels aplicatius i dades anteriors a ‘’l’atac’’.

Acabem de comprovar de forma directa, que un hipotètic atac amb un dispositiu sense suport, no actualitzat o bé, que utilitzi un protocol vulnerable pot arribar a suposar pèrdua de dades.

3.2. Proves de connexió en entorn obert

En aquesta fase de l’estudi, es realitzarà un rastreig de dispositius en un entorn obert ubicat a la ciutat de Barcelona amb l’objectiu de servir com a base a l’informe d’auditoria final. Concretament es vol:

- Conèixer quins tipus de dispositius hi ha a la nostra ubicació.
- Comprovar la seguretat als dispositius identificats dels usuaris col·laboradors.

En aquest cas, la comprovació consistirà si el dispositiu del col·laborador pot rebutjar o no, intents de connexió (emparellament) seguits, tal com es faria en una situació DoS. En cap moment es tractarà d’accedir de forma deliberada al contingut del dispositiu o qualsevol altre desconegut. Si més no, es possible que s’incrementi temporalment el consum de la bateria del dispositiu estudiat com a conseqüència del procès de connexió i rebuig.

3.2.1. Dispositius Bluetooth BR

Iniciem el rastreig de dispositius Bluetooth BR amb el mòdul Bluetooth Intel integrat al equip que integra la plataforma d’anàlisi:

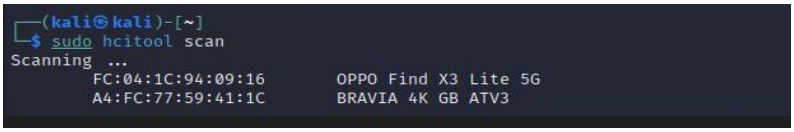

Figura 21. Entorn obert. Resultat comanda *sudo hcitool scan*

Figura 22. Entorn obert. Resultat comanda *sudo hcitool scan --info*

Es detecten dos dispositius que fàcilment s'identifiquen. En el cas del televisor Sony Bravia Smart TV, s'identifica com Mediatek ja que la comanda ens mostra la informació del SoC (CPU interna de gestió) que s'utilitza en alguns models de televisors del fabricant Sony que funcionen sota una versió adaptada del sistema operatiu Android[12]

El segon dispositiu detectat es tracta d'un telèfon del fabricant Oppo. Donat que la persona propietària col·labora amb aquest estudi, farem un intent simple de connexió des de el propi gestor de connexions Bluetooth de Kali (BlueManager). En aquest cas, triant el dispositiu i amb el menú contextual, triant l'opció *«pair»*

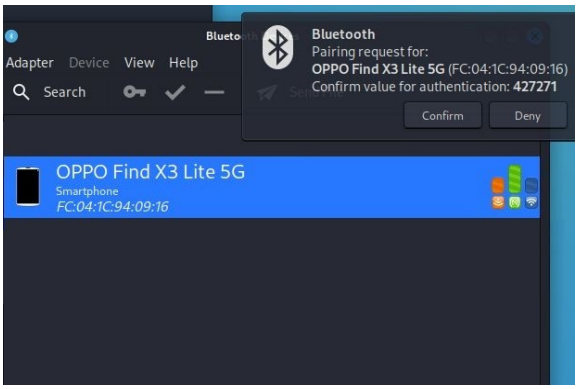

Figura 23. Comprovació de seguretat. Emparellament amb BlueManager

Es pot comprovar que el dispositiu accepta la connexió sense problemes i es podria emparellar confirmant el PIN d'autentificació. En aquest cas, tenim un exemple d'una configuració molt poc segura al mantenir sempre la connexió oberta i fer el dispositiu visible a tothom, però «còmoda» des de el punt de vista de l'usuari.

3.2.2. Dispositius BLE

Es repeteix el rastreig per a dispositius BLE, amb la comanda:

```
sudo hcitool lescan
```

```
┌──(kali㉿kali)-[~]
└─$ sudo hcitool lescan
LE Scan ...
3B:3B:39:E6:32:63 (unknown)
2F:03:B7:25:99:FC (unknown)
53:E4:18:10:D6:9C (unknown)
FF:05:01:0B:2E:77 Fulife
A4:FC:77:59:41:1C (unknown)
A4:FC:77:59:41:1C (unknown)
FF:05:01:0A:18:94 Fulife
18:B9:05:C7:FA:CC (unknown)
18:B9:05:C7:FA:CC LEDnetWF010033C7FACB
7D:9D:ED:38:CC:A2 (unknown)
FF:05:01:0A:18:94 (unknown)
7D:9D:ED:38:CC:A2 (unknown)
FF:05:01:0B:2E:77 (unknown)
4F:50:29:30:91:F7 (unknown)
4F:50:29:30:91:F7 (unknown)
66:6F:91:5A:BA:5C (unknown)
CA:47:E6:16:10:51 (unknown)
8C:CE:FD:17:DC:1A (unknown)
8C:CE:FD:17:DC:1A Mi Smart Band 4C_DC1A
D7:08:06:7E:7A:A2 (unknown)
ED:0A:51:9F:74:13 (unknown)
ED:0A:51:9F:74:13 Forerunner 235
70:B0:1E:79:A6:ED (unknown)
D7:3C:B4:95:AB:F5 (unknown)
E6:85:8B:67:24:F1 (unknown)
42:54:6C:AC:4B:40 (unknown)
42:54:6C:AC:4B:40 (unknown)
1C:DA:04:4C:44:BF (unknown)
FD:93:2A:CB:55:F2 (unknown)
45:7E:1C:A7:F7:E1 (unknown)
11:77:48:00:AB:CA (unknown)
```

Figura 24. Resultat comanda *sudo hcitool lescan*

12 Informació i característiques Android TV: https://www.android.com/tv/

Obrint Wireshark, podem veure el tràfic generat i capturar la informació dels paquets per a un estudi posterior. En aquest anàlisi, també es fa servir el mòdul Bluetooth estàndard Intel de l'equip amfitrió:

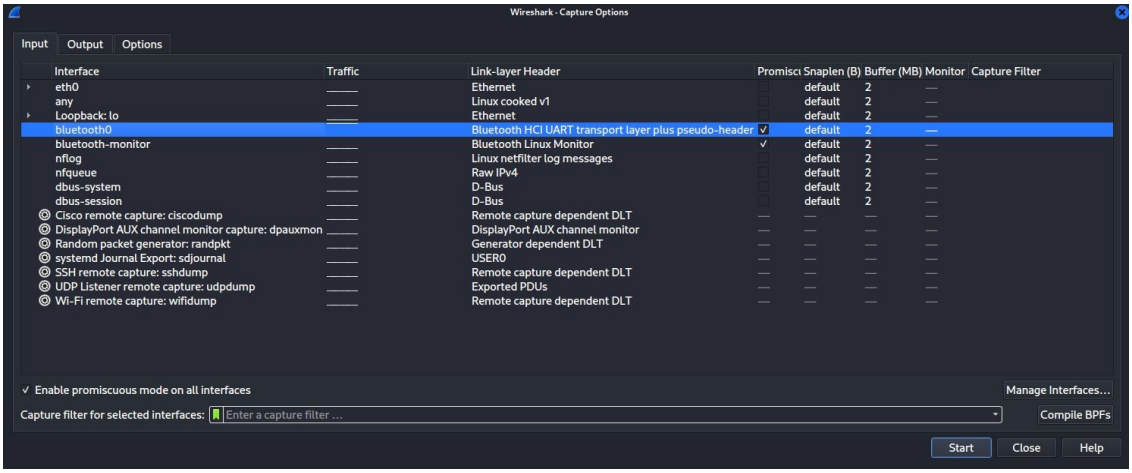

Figura 25. Configuració Wireshark per Bluetooth interna (Intel)

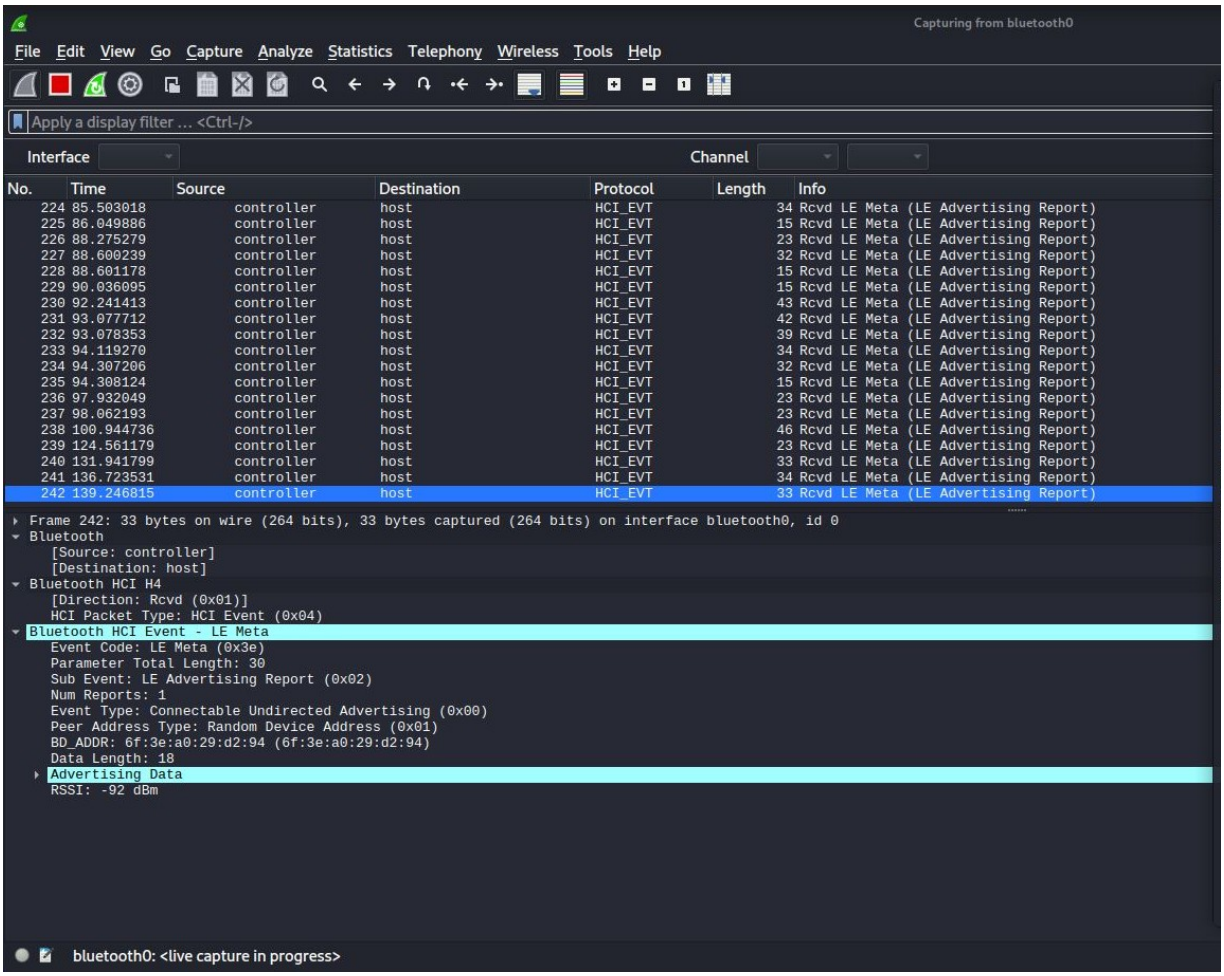

Figura 26. Wireshark amb tràfic de *sudo hcitool lescan*

Donat que hi ha més dispositius i el procès es més lent, es deixa un temps capturant dades. Al cap de 30 minuts, s'atura l'execució de la comanda. Es capturen al voltant de 18000 paquets.

Dins de Wireshark, s'activa el filtrat que ens mostra quins dispositius s'han trobat i netejar els paquets originats per interferències o errors:

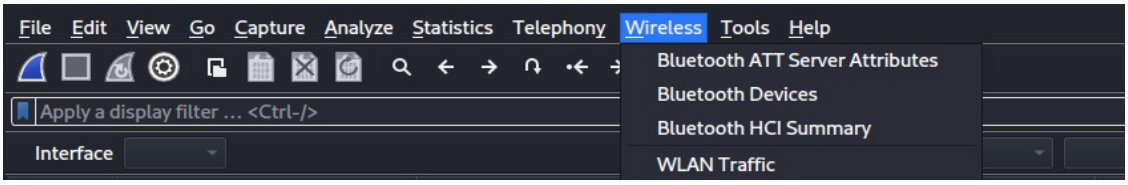

Figura 27. Filtrat dispositius Bluetooth a Wireshark.

S'informa que s'han trobat 282 elements. La figura 27 mostra una part d'aquests dispositius. Podem comprovar que hi ha dispositius molt variats, des de portables (Mi Smart Bands, Forerunner 235), auriculars fins dispositius IoT (sistemes d'enllumenament LEDnet, sistemes de mans lliures..)

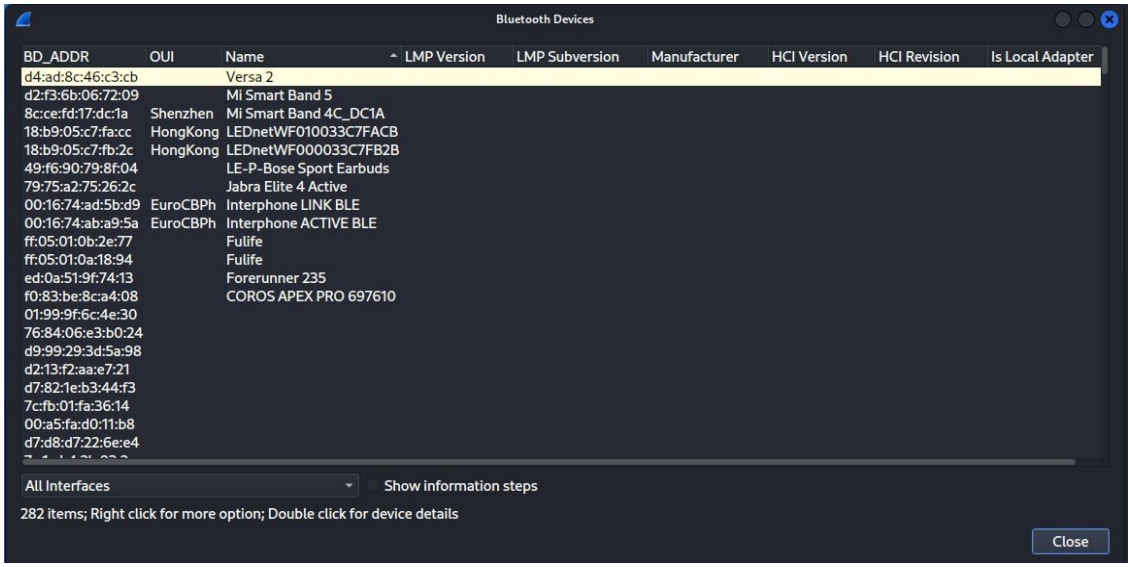

Figura 28. Dispositius Bluetooth BLE detectats a Wireshark

Executem des de terminal, la comanda per que ens mostri més informació d'un dispositiu determinat. En aquest cas, triem les MAC ED:0A:51:9F:74:13 (Garmin Forerunner 235) que correspon al dispositiu portable Garmin Forerunner 235 i del punt de llum LEDNet amb MAC 18:B9:05:C7:FA:CC

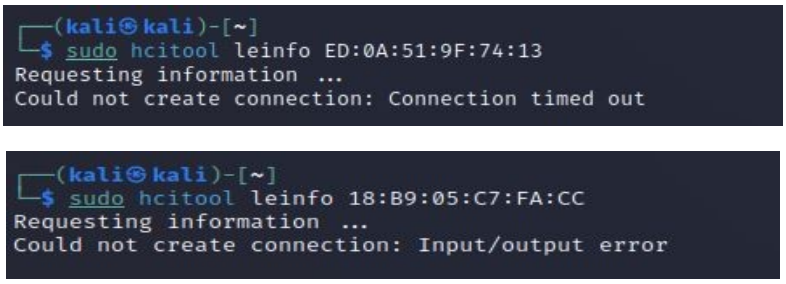

Figura 29. Resultat comanda sudo hcitool leinfo

Comprovem que tots dos dispositius rebutgen mostrar més informació. En el cas del dispositiu Forerunner, dona un error de temps d'espera.

Altrament, al dispositiu IoT LEDNet, hi ha resposta però per problemes de connexió (paquets mal formats), la comanda no finalitza amb les dades sol·licitades.

3.2.3. Anàlisi mitjançant Ubertooth

Es repeteix el rastreig, però amb el dispositiu Ubertooth. Prèviament, es crea un canal (pipe) amb la comanda `mkfifo /tmp/port_ubertooth_one` per que Ubertooth One pugui enviar el tràfic que va capturant a Wireshark i aquest, el processi.

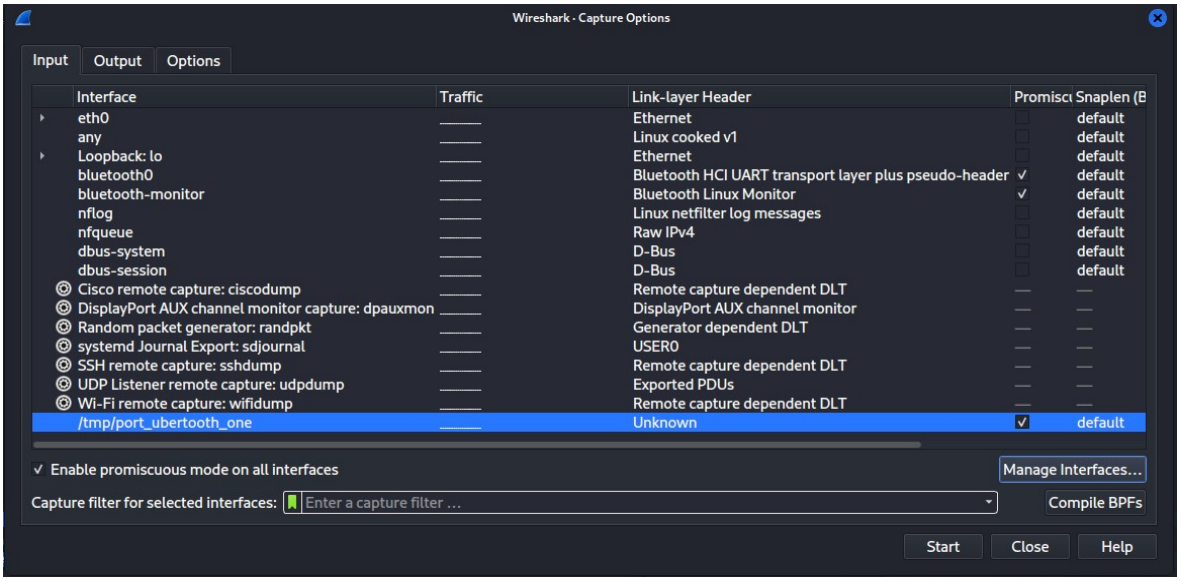

Figura 30. Configuració Wireshark per Ubertooth One

S'executa la comanda `ubertooth-btle -f -c /tmp/port_ubertooth_one` i Ubertooth One, comença a capturar i reenviar el tràfic detectat a Wireshark:

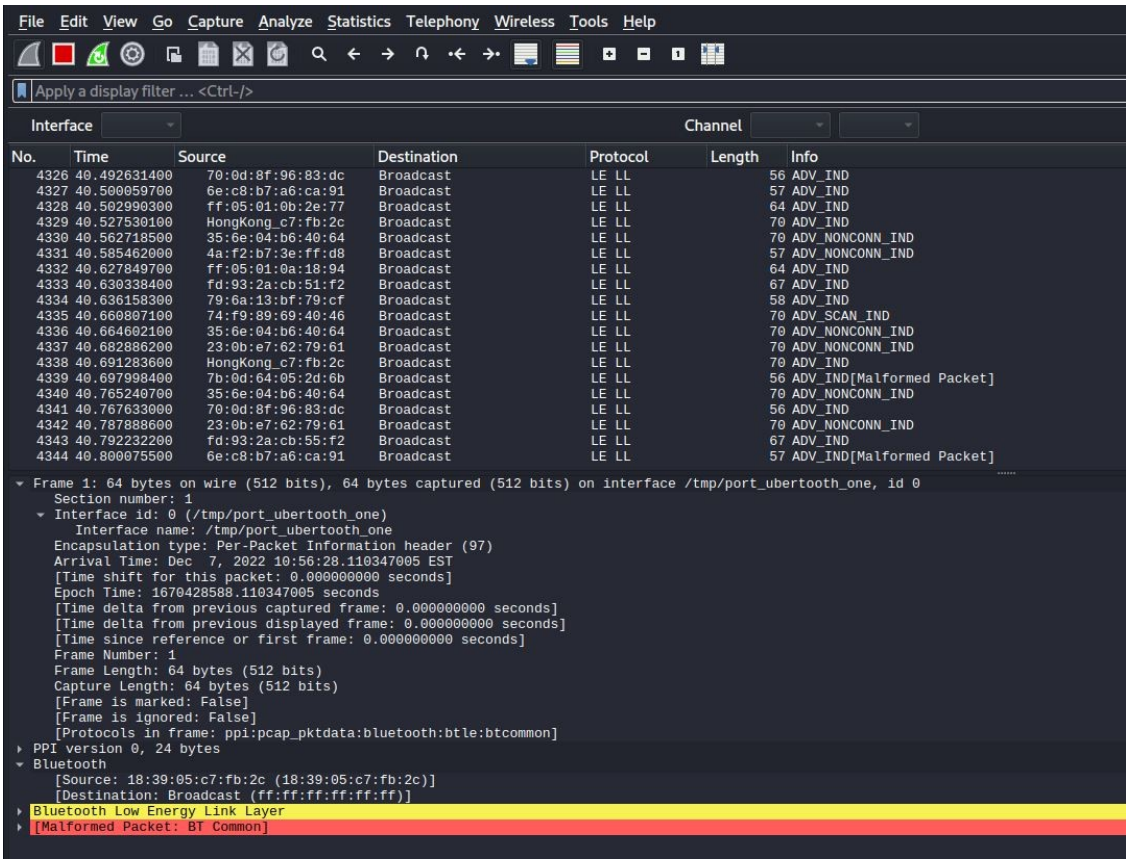

Figura 31. Wireshark amb tràfic de *ubertooth-btle -f -c /tmp/port_ubertooth_one*

La velocitat de procès i de captura de paquets es significativament molt més ràpida. De fet, es tanca manualment la captura de paquets al cap de 10 minuts d'iniciar la prova ja que hi ha més de 50.000 paquets recopilats. Analitzant la informació capturada, es detecten 1768 dispositius. La figura 32 mostra un llistat amb alguns dels dispositius detectats.

La diferencia notable de rendiment entre els tots mòduls Bluetooth, s'explica a que Ubertooth es una eina específica, tan per a la seva part de maquinari com a la de programari, per aquestes tasques. Integra la seva pròpia CPU i electrònica de procès de senyal i no ha de dependre de l'amfitrió per processar les dades, llevat de la transmissió de les dades mitjançant USB amb l'amfitrió.

Per altre banda, el dispositiu disposa d'una antena dedicada amb un guany molt superior a la convencional dels equips portàtils. Donat que Ubertooth es un dispositiu de classe I, ens permet detectar dispositius en 100 metres al voltant. Per qüestions de privacitat, només es mostren els tres primers dígits de les MAC detectades.

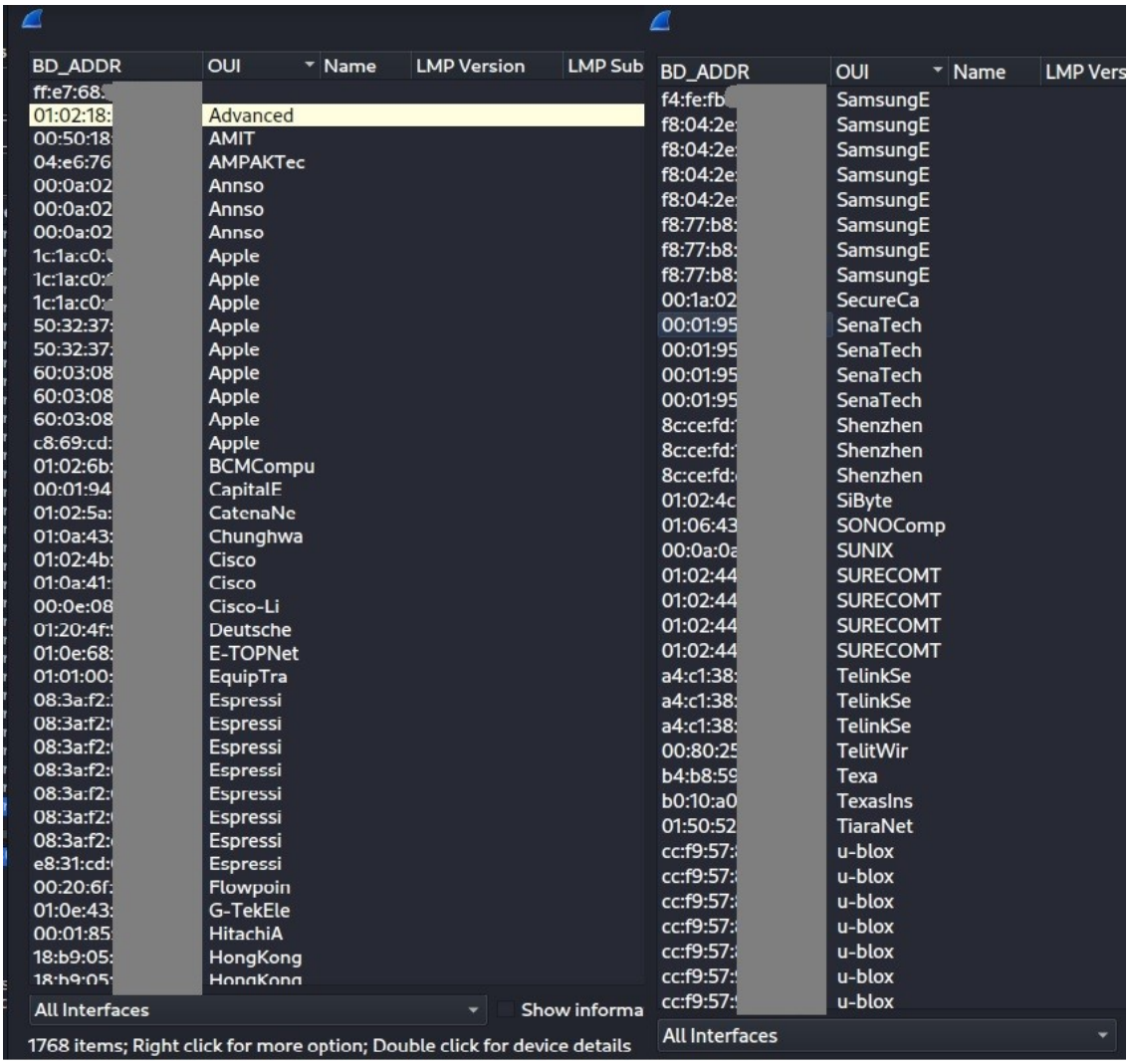

Figura 32. Dispositius Bluetooth BLE detectats a Wireshark amb Ubertooth

En aquest cas, es posa de manifest que de forma relativament senzilla, un hipotètic atacant podria descobrir, obtenir i capturar massivament múltiples MAC (BD-ADD) de dispositius Bluetooth sense necessitat de estar físicament a prop. Per temes de seguretat i privacitat, no es fa cap prova amb aquests dispositius que a més, no participen de forma directa a l'anàlisi.

Seguidament es realitza una prova d'anàlisi amb les eines integrades amb Ubertooth amb un dispositiu determinat. Es vol analitzar la banda d'activitat Smartband 4C del fabricant Mi (Xiaomi), molt popular pel seu baix cost i prestacions acceptables per al públic en general.

La raó de triar aquest dispositiu i no altre, es la comprovar la seguretat del dispositiu, atès que al estudi [2] *Security and privacy threats for bluetooth low energy in IoT and wereable devices*. (Barua et al), Volume 3 2022, pg 272, D - Hack smart band, es deixa en evidencia la poca seguretat d'aquests models de dispositius.

Fent servir el gestor de connexions Bluetooth de Kali (BlueManager), es realitza un intent de connexió amb el dispositiu amb la adreça 8C:CE:F0:17:DC:1A (SmartBand 4C), que es va detectar anteriorment i que forma part de la prova general. En aquest cas, es segueix el procès des de Wireshark:

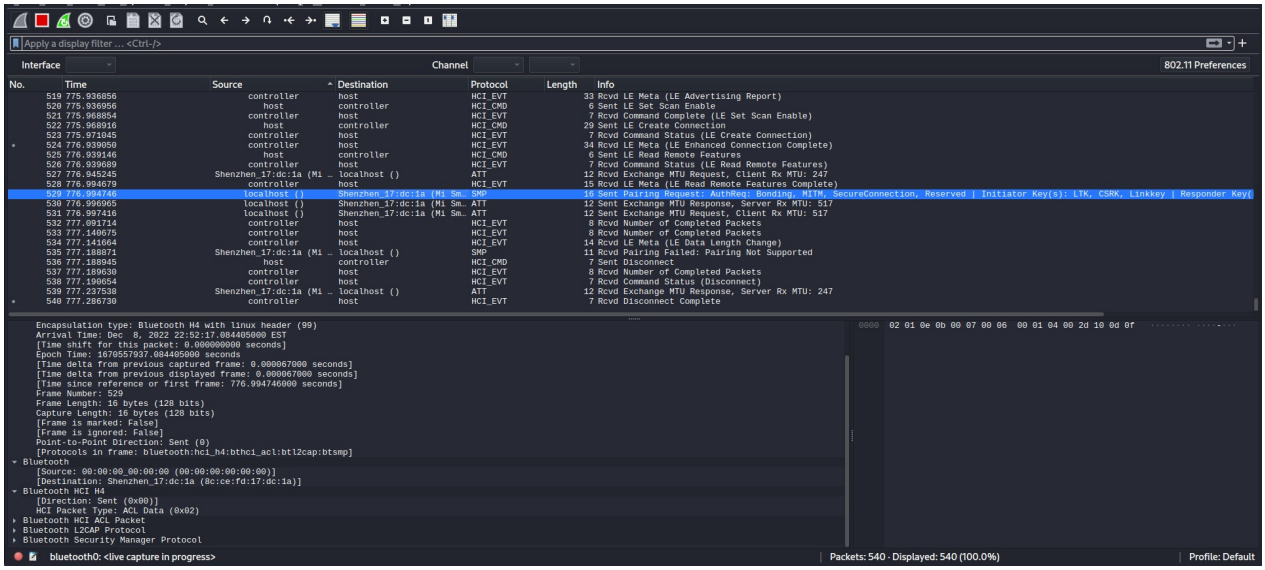

Figura 33. Trames connexió Wireshark

Més en detall, es comprova que a la trama 522 s'inicia l'intercanvi de dades entre l'equip auditor i el dispositiu, negociant la connexió:

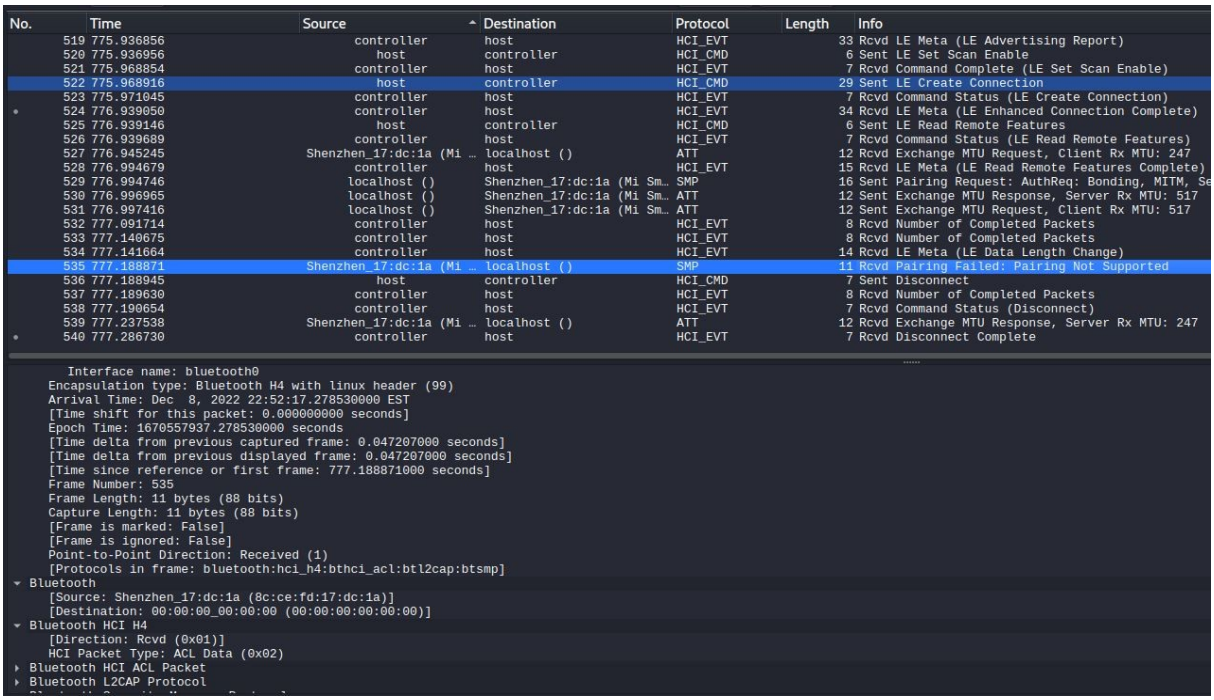

Figura 34. Trama desconnexió Wireshark

Es comprova que el dispositiu, a diferencia del cas del dispositiu Oppo, finalment rebutja la connexió a la trama 535 i a la 540 es tanca la connexió entre tots dos dispositius:

525	776.939146	host	controller	HCI_CMD	6 Sent LE Read Remote Features
526	776.939689	controller	host	HCI_EVT	7 Rcvd Command Status (LE Read Remote Features)
527	776.945245	Shenzhen_17:dc:1a (Mi …	localhost ()	ATT	12 Rcvd Exchange MTU Request, Client Rx MTU: 247
528	776.994679	controller	host	HCI_EVT	15 Rcvd LE Meta (LE Read Remote Features Complete)
529	776.994746	localhost ()	Shenzhen_17:dc:1a (Mi Smart Band 4C_DC1A)	SMP	16 Sent Pairing Request: AuthReq: Bonding, MITM, Se
530	776.996965	localhost ()	Shenzhen_17:dc:1a (Mi Smart Band 4C_DC1A)	ATT	12 Sent Exchange MTU Response, Server Rx MTU: 517
531	776.997416	localhost ()	Shenzhen_17:dc:1a (Mi Smart Band 4C_DC1A)	ATT	12 Sent Exchange MTU Request, Client Rx MTU: 517
532	777.091714	controller	host	HCI_EVT	8 Rcvd Number of Completed Packets
533	777.140675	controller	host	HCI_EVT	8 Rcvd Number of Completed Packets
534	777.141664	controller	host	HCI_EVT	14 Rcvd LE Meta (LE Data Length Change)
535	777.188871	Shenzhen_17:dc:1a (Mi …	localhost ()	SMP	11 Rcvd Pairing Failed: Pairing Not Supported
536	777.188945	host	controller	HCI_CMD	7 Sent Disconnect
537	777.189630	controller	host	HCI_EVT	8 Rcvd Number of Completed Packets
538	777.190654	controller	host	HCI_EVT	7 Rcvd Command Status (Disconnect)
539	777.237538	Shenzhen_17:dc:1a (Mi …	localhost ()	ATT	12 Rcvd Exchange MTU Response, Server Rx MTU: 247
540	777.286730	controller	host	HCI_EVT	7 Rcvd Disconnect Complete

Figura 35. Trama desconnexió dispositius a Wireshark

En aquest cas, podem dir que el dispositiu Smartband 4C té un mínim de seguretat configurada, ja que tot i que estigui visible, rebutja la connexió d'un dispositiu no emparellat prèviament.

Amb el el mateix dispositiu detectat (Mi Smartband 4C), farem un segon experiment però fent servir les eines específiques Ubertool. Duplicarem la seva adreça MAC i comprovarem si el dispositiu amfitrió (telèfon Nokia 9 basat en Android 10), pot establir la connexió amb el dispositiu. Es planteja aquest escenari:

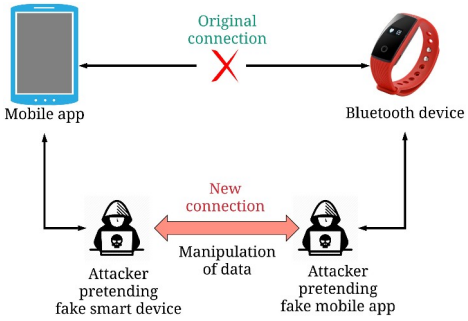

Figura 36. Man-In-The-Middle attack
Font i origen imatge: [2] BARUA et al.: SECURITY AND PRIVACY THREATS FOR BLUETOOTH LOW ENERGY IN IoT AND WEARABLE DEVICES. Volume 3 2022, pg 261

Per aquesta segona prova ens cal que inicialment desconnectem la polsera d'activitat del amfitrió. Posteriorment, des de Kali executem aquesta comanda des de una consola de terminal:

```
ubertooth-btle -s 8C:CE:FD:17:DC:1A
```

Aquesta comanda, tal com es va realitzar a la prova amb el dispositiu de prova Palm, fa que el dispositiu Ubertooth comenci a emetre paquets amb la mateixa MAC que el dispositiu original.

Des de el gestor de connexions Bluetooth de Kali, seguim detectant el dispositiu. Intentem establir la connexió entre tots dos i emparellar-los manualment l'equip virtual al dispositiu:

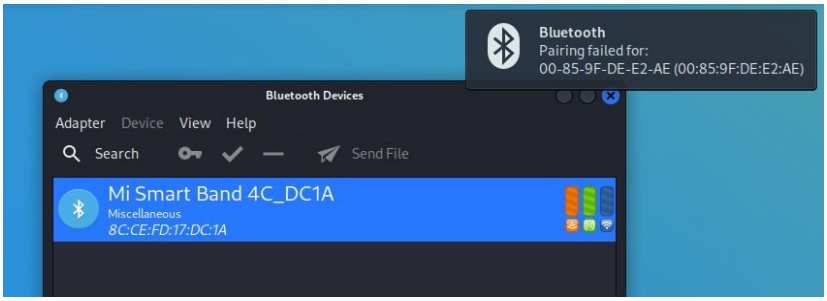

Figura 37. Connexió a dispositiu BLE

Tot i que s'estableix connexió entre l'equip virtual i la Smartband (no mostra la icona d'error de connexió), no es possible emparellar-los.

Comprovem que el dispositiu clonat es detecta també des de el dispositiu amfitrió (Nokia 9). A priori, no tenim cap sospita que pugui existir altre dispositiu *Mi Smart Band 4C_DC1A*

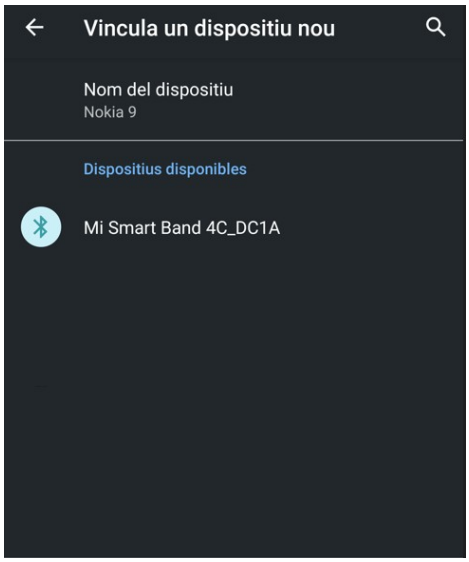

Figura 38. Dispositiu clonat

Des de el dispositiu amfitrió, s'executa l'aplicació de gestió *MI Fitness* per sincronitzar les dades entre tot dos dispositius i es comprova que no es pot establir la connexió tot i que està actiu:

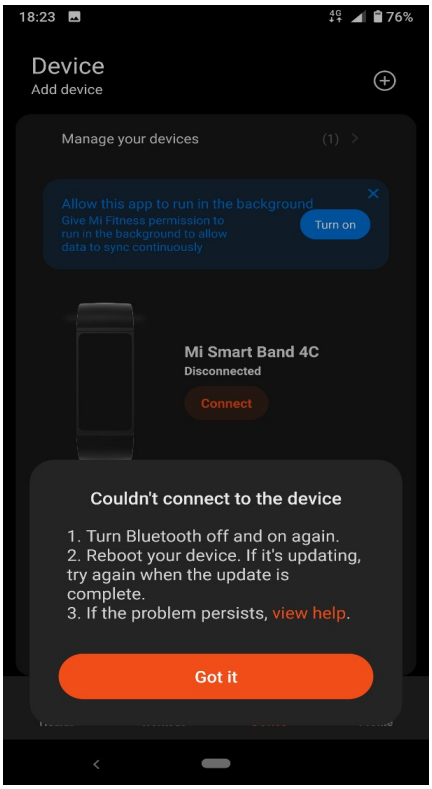

Figura 39. Bloqueig d'emparellament

S'ha provocat un bloqueig amb els dispositius originals emparellats en tenir dos dispositius amb la mateixa MAC (el autèntic i el virtual generat des de Kali), que interfereix la connexió. L'efecte es molt similar a una situació d'atac de denegació de servei (DoS).

Per sortit d'aquesta situació de bloqueig, només cal tancar el dispositiu «fals» a Kali i reiniciar l'aplicació a l'amfitrió.

4. Conclusions i treballs futurs

En aquest capítol, es presenten les conclusions d'aquest treball, així com altres qüestions presentades durant el desenvolupament.

4.1. Conclusions

L'objectiu d'aquest treball era comprovar la seguretat que ofereixen diferents dispositius portables amb el punt més feble que el podem trobar amb la connexió per intercanviar dades amb altres dispositius. En aquest cas, s'ha focalitzat a la tecnologia Bluetooth.

S'han comprovat dues situacions on es posen de manifest alguns dels problemes descrits:

- Problemes de seguretat generats per sistemes obsolets i sense suport per part del fabricant. Aquest es el cas de l'experiment amb la PDA Palm.

- Problemes de seguretat generats per configuració poc adequada del dispositiu. En aquest cas, es comprova que sense fer ús d'eines especifiques d'atac, hi han dispositius que accepten la connexió de dispositius no emparellats prèviament. En altres, s'aconsegueix interferir la connexió dels dispositius.

Tot i així, també s'han detectat altres casos on els dispositius detectats no emparellats, rebutgen els intents de connexió.

Per altre banda, s'experimentat la possibilitat i risc real de patir una situació molt similar de denegació de servei. Especialment en dispositius de baix cost amb poca capacitat de processament, on es possible interferir la connexió.

Com a conclusió, Bluetooth possibilita la interacció de múltiples sistemes i dispositius fàcilment, però requereix també la conscienciació dels usuaris sobre els riscos de seguretat. Bastaria només activar la comunicació en el moment de la seva utilització, tot i que s'ha pogut comprovar que en alguns dispositius de baix cost no es possible desactivar aquesta funció.

Finalment, amb aquestes dades podem fer un informe a mode de resum de les dades obtingudes. Al següent apartat, es mostra com seria aquest informe.

4.1.1. Informe auditoria

Data: gener 2023

Ubicació: instal·lacions oficines client, a Barcelona centre.

Mètodes:
- Captura de tràfic i detecció de dispositius Bluetooth mitjançant plataforma portàtil.
- Escaneig del dispositiu.

RESULTATS

Dispositius portables i IdC detectats (Bluetooth BR / BLE) dins de la ubicació:

Dispositiu	Identificació /Fabricant	Connexió oberta ?	Actualització programari
TV Sony Bravia	Si / Sony Corp.	Si. Però es rebutja al connectar-se.	Web fabricant
Telèfon Oppo Find X3 Lite 5G	Si /Oppo	Si	Mitjançant app
Banda d'activitat Mi SmartBand 4C	Si / Mi (Xiaomi)	No	Mitjançant app
Rellotge Garmin Forerunner 235	Si / Garmin inc.	No	Web fabricant /app
Il·luminaria LedNet	Si / Hong Kong Bouffalo Lab Limited*	No	n/c

*Determinat per recerca a la bbdd de https://mac.lc/

Proves específiques:
Banda d'activitat Mi SmartBand 4C: duplicació de BR-ADDR, bloquejant la connexió amb el dispositiu amfitrió.

Observacions:
- Configuració sense cap seguretat: es detecta com a mínim un dispositiu sense cap protecció que permet l'emparellament. (Oppo Find X3)

- S'aconsegueix interferir en la connexió d'un dispositiu portable. (MI Smartband 4C).

Recomanacions:
Els problemes de seguretat detectats, poden ser fàcilment corregits fent que els dispositius sempre estiguin emparellats, mantenint la connexió Bluetooth activada només quan sigui necessari.

Alguns dels dispositius, no integren les últimes actualitzacions de programari publicats per fabricant.

4.2. Assoliments dels objectius plantejats

Amb la metodologia emprada -captura de dades amb una plataforma portàtil i virtual dissenyada i construïda per aquest propòsit-, s'han assolits els objectius principals que eren el poder analitzar dispositius en un entorn real de funcionament. Tot i així, degut a qüestions de temps, s'ha tingut que reduir les sessions de recopilació de dades, així com la quantitat de dispositius a analitzar.

També s'aprofunditt coneixements amb temes de ciberseguretat i funcionament dels sistemes amb connectivitat Bluetooth: funcionament, vulnerabilitats, exploits.

4.3. Seguiment de la planificació

La planificació inicial s'ha tingut que modificar, ja que per alguns temes s'ha tingut que resumir molta informació. Només cal fer una ullada al web de SIG Bluetooth on es pot consultar qualsevol implementació, norma del protocol de forma molt extensa.

Altre factor important ha sigut el compaginar aquest treball amb altres assignatures, que ha restat temps dedicat. Això s'ha traduït que algunes proves de testeig previstes al segon lliurament (PAC 2) amb la plataforma d'anàlisi, s'han desplaçat al següent lliurament.

Amb la metodologia emprada, s'han assolits els objectius principals que eren el poder analitzar dispositius en un entorn real de funcionament amb el major número de dispositius possibles.

4.4. Impactes

Durant el procès d'elaboració d'aquest treball, s'han plantejat varies qüestions sobre la seguretat amb els dispositius portables i de retruc, amb els dispositius IdC (IoT). S'ha constatat que sense massa dificultat, es possible bloquejar un dispositiu o bé, generar interferències durant el seu ús. Un dels objectius d'aquest treball es poder servir com a base per poder implementar bones pràctiques, conscienciar als usuaris i evitar riscos de seguretat.

En les situacions descrites, hi ha certa complicitat amb els usuaris col·laboradors ja que se'ls informa prèviament i en cas de trobar alguna anomalia es comenta a final de la prova. Aquest tipus de prova, algunes empreses dedicades a la ciberseguretat se'ls anomena com *anàlisi de caixa blanca.*

Tot això ens fa reflexionar davant la situació si, en comptes d'analitzar polseres d'activitats, rellotges o telèfons, els dispositius fossin sistemes crítics com podem trobar a hospitals o laboratoris. Podem patir un impacte negatiu amb greus conseqüències. Resulta molt inquietant, tal com es recull en el treball

d'investigació *Exploiting Bluetooth Vulnerabilities in e-Health IoT Devices*, Zubair et al. 2019[6], també amb Ubertooth One, on es demostra les possibles vulnerabilitats i atacs cap a dispositius mèdics IdC per monitorar als pacients.

Amb aquest nou escenari, s'han fet consultes a tres fabricants o distribuïdors de sistemes que integren connectivitat Bluetooth amb els quals aquest autor té relació professional.

Davant la pregunta *si en algun dels vostres productes està o no implementada aquesta tecnologia i si ho està, quines mesures de protecció -sense entrar en detalls -s'han establert,* la resposta dels col·laboradors (citats a l'annex) ha sigut:

- Un col·laborador opta no implementar aquesta tecnologia. Alternativament, s'utilitzen solucions cablejades punt a punt, securitzades.

- Altres col·laboradors l'implementen, però amb limitacions d'ús per mitigar els problemes de seguretat descrits en aquest treball:

    - Requeriment d'un dispositiu propietari per enllaçar els dispositius. Ex: mesuradors de glucosa en sang emparellat al telèfon de l'usuari.

    - Conversió de la connexió Bluetooth a NFC, que força la connexió a pocs centímetres. Ex.: sistemes de control horari, controls de presencia...

4.4.1. Marc Legal

Una de les raons de l'elaboració d'aquest treball, va ser motivada sobre la polèmica en Estats Units envers la llei d'avortament aprovada a mitjans de 2022. Es plantejava si en un moment donat, davant de sospites d'avortaments en estats on es il·legal, algú -asseguradores-, podia accedir a les dades biomètriques de dones que feien servir les funcions de registre menstrual o apps de fertilitat, dels seus rellotges intel·ligents i bandes d'activitat.

Segons el marc actual a la UE -Reglament Europeu (RGPD 2016/679)-, les lleis que regulen l'accés les dades personals son molt més restrictives. Es consideren un dret fonamental. La situació que es va plantejar als Estats Units no té cap cabuda actualment. Qualsevol captura de dades d'aquest tipus seria il·legal, i a més amb sancions econòmiques considerables.

Aquests temes van ser tractats dins de l'article i debat a la UOC, de la periodista Núria Meseguer «*Les apps menstruals a debat després de l'abolició de l'avortament als EE.UU: com afecta a Espanya*?»[13]

13 21/07/2022. Núria Meseguer Ferré, «Les apps menstruals a debat després de l'abolició de l'avortament als EE.UU: com afecta a Espanya?» https://www.uoc.edu/portal/ca/news/actualitat/2022/189-apps-control-menstrual-abortament.html
Data consulta: setembre 2022

4.5. Línies de treball futur

La nova implementació del protocol Bluetooth (5.3), integra noves funcions de seguretat i encriptació millorada de les comunicacions del dispositius. Aquests, cada vegada disposen de major capacitat de processament que els hi permeten suportar millores a l'àmbit de seguretat. Es podria fer un estudi amb dispositius amb major robustesa i comprovar aquesta fita.

Altres punts de estudi dins de la seguretat informàtica, estaria enfocat als dispositius industrials. Es podria adaptar aquest treball cap a l'industria 4.0 i estudiar la seguretat que integren alguns dispositius, així com la seva robustesa enfront a hipotètics atacs. Cal recordar situacions [14] com va succeir a la xarxa elèctrica d'Ucraïna a finals de 2016, on presumptament un ciberatac dirigit cap a un distribuïdor local, va bloquejar el sistemes de gestió de subministrament elèctric atacant els dispositius IoT no actualitzats (convertidors serie-ethernet), que monitoritzen les dades de les subestacions.
Com a resultat, es van generar greus problemes a la població deixant sense servei per unes hores a tota una regió en ple hivern.

14 Ciberatac a la xarxa elèctrica d'Ucraïna https://www.incibe-cert.es/blog/nuevo-ciberataque-red-electrica-ucrania. Data consulta 9 desembre 2022

5. Glossari

Definició dels termes i acrònims més rellevants utilitzats dins la Memòria.

BLE: Abreviatura de *Bluetooth Low Energy,* Bluetooth de baix consum. Versió de baix consum de la tecnologia Bluetooth, dissenyada principalment per l'ús a dispositius alimentats amb bateries o piles: sensors, polseres d'activitat, dispositius Iot.

BR/ EDR: Abreviatura de *Basic Rate / Enhaced Date Rate.* Versions estàndard de la tecnologia Bluetooth, orientades per a transmetre gran quantitat de dades. Per contra, té un consum energètic més elevat en comparació a BLE.

DoS: acrònim anglès *Denial of Service.* Ciberatac consistent en saturar un servidor mitjançant connexions massives fins a bloquejar-lo o provocar una resposta molt lenta dels serveis que ofereix als usuaris.

Emparellament (paired): establiment inicial de la connexió i configuració entre dispositius Bluetooth.

IEEE: acrònim anglès *Institute Electrical and Electronics Engineers (*Institut d'Enginyers Elèctrics i Electrònics. Associació mundial sense ànim de lucre dedicada a la normalització i desenvolupament de les àrees tècniques a les enginyeries relacionades amb les tecnologies de la informació.
Web oficial: https://www.ieee.org/

Iot: acrònim anglès *Internet of Things*. En català, IdC: Internet de les coses. Xarxa de dispositius intel·ligent -sensors industrials, mediambientals, sistemes d'enllumenament, electrodomèstics-, interconnectats per intercanvi i recollida de dades dels seu entorn.

ISM: acrònim anglès *Industrial, Scientific and Medical*. Banda de radio freqüències reservades a nivell internacional per usos industrials, científics i mèdics.

MiTM: acrònim anglès *Man in The Middle.* Ciberatac consistent en la captura de les dades que es transmeten dos dispositius per a poder interferir o manipular les dades que s'intercanvien.

NFC: acrònim anglès Near Field Communications, (Comunicació de camp proper). Tecnologia sense fils que fa servir petits camps magnètics, que permet intercanvi de dades entre dispositius que estiguin a molt poca distancia (pocs centímetres).

PDA: Personal Digital Assistant. (Assistent personal digital o agenda digital). Predecessor dels actuals telèfons mòbils al principi, es un petit ordinador de butxaca orientat com agenda o organitzador personal i amb possibilitat d'executar aplicacions específiques varies. Es sincronitza amb l'ordinador de l'usuari, te connectivitat sense fils i reconeixement de l'escriptura amb pantalla tàctil.

Amb l'arribada i popularització dels telèfons intel·ligents que integraven aquestes funcions a més de connexió a Internet, trucades i altres, van caure en desús.

Sniffer (detector): Programa situat en un servidor d'una xarxa que controla i analitza els paquets i fitxers que hi circulen i n'extreu informacions. *Definició a (https://www.termcat.cat/ca/cercaterm/sniffer?type=basic). Data consulta 8 de gener 2023.*

Wearable device / Dispositiu portable: petit dispositiu electrònic dissenyat per poder ser integrat dins de la roba o altres complements dels usuaris com rellotge intel·ligent, banda d'activitat o fins i tot a dispositius mèdics. Permet monitoritzar diferents constants biomètriques de les persones.

6. Bibliografia i col·laboracions

Fonts consultades i citades en aquest treball

[1] Dades i web oficial de Bluetooth SIG:
https://www.bluetooth.com/
Data consulta: octubre-novembre 2022

[2] A. Barua, M. A. Al Alamin, M. S. Hossain and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," in *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251-281, 2022, doi: 10.1109/OJCOMS.2022.3149732.
Disponible a:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9706334&isnumber=9702748
Data consulta: octubre-novembre 2022

[3] L. Raya, ‘’La seguridad en Bluetooth’’
https://www.acta.es/medios/articulos/ergonomia_y_seguridad/053049.pdf
ACTA. *Asociación de Autores Científico-Técnicos y Académicos*.
Data consulta: octubre-novembre 2022

[4] Documentació projecte Ubertooth:
https://github.com/greatscottgadgets/ubertooth
Data consulta: octubre-novembre 2022

[5] Documentació Kali: https://www.kali.org/docs/
Eines i utilitats: https://www.kali.org/tools/
Data consulta: octubre-desembre 2022

[6] M.Zubair, D. Ünal, A.K. Al-Ali, A. Shikfa
‘’Exploiting Bluetooth Vulnerabilities in e-Health IoT Devices’’ Conference: 3rd International Conference on Future Networks and Distributed Systems (ICFNDS ’19) At: Paris, France
Disponible a:
https://www.researchgate.net/publication/334524460_Exploiting_Bluetooth_Vulnerabilities_in_e-Health_IoT_Devices
Data consulta: octubre 2022

[7] Termcat. Centre de terminologia: diccionari i recursos lingüístics a les TIC.
https://tic.termcat.cat/ca
Data consulta: octubre 2022 - gener 2023

Fonts addicionals consultades:

Security Issues in Bluetooth Networkes (Section VIII):
S. Baraković et al., "Security issues in wireless networks: An overview," 2016 XI International Symposium on Telecommunications (BIHTEL), 2016, pp. 1-6, doi: 10.1109/BIHTEL.2016.7775732.
Disponible a:
https://ieeexplore.ieee.org/abstract/document/7775732?casa_token=t7h4aW8HrK4AAAAA:Z9VErUSEzboOvmO0wZJq7-nVQkiMJS2CD0XtXmBfHvK_SmEN7Sc5X78DiPR35Sja4tPYCchzwg
Data consulta: octubre 2022

Nordic Solutions. Funcionament encriptació AES-CCM a Bluetooth 4.0
https://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.nrf52832.ps.v1.1%2Fccm.html
Data consulta: octubre 2022

Marc legal a la UE. Data consultes: octubre-desembre 2022

Llei de protecció i tractament de dades dels ciutadans de la UE
https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04?locale=es

Comitè Europeu de protecció de dades:
https://edpb.europa.eu/edpb_es

La protecció de dades a la UE:
https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es#:~:text=El%20Reglamento%20general%20de%20protecci%C3%B3n%20de%20datos%20(RGPD)&text=El%20Reglamento%20es%20una%20medida,en%20el%20mercado%20%C3%BAnico%20digital.

Tractament de dades biomètriques:
https://www.datax.es/blog-actualitat-proteccio-dades/ca/dictamen-de-lapdcat-sobre-el-reconeixement-facial/
Data consulta: 9 gener 2023

APDCAT: Autoritat Catalana de Protecció de Dades
https://apdcat.gencat.cat/ca/drets_i_obligacions/rgpd/
Data consulta: octubre 2022

INCIBE: Instituto Nacional de Ciberseguridad de España
https://www.incibe-cert.es/blog/iot-protocolos-comunicacion-ataques-y-recomendaciones
Data consulta: octubre 2022

Fonts d'informació addicionals. Col·laboracions

Aquestes empreses han col·laborat aportant informació i temes de seguretat sobre determinats dispositius que comercialitzen o fabriquen amb connectivitat Bluetooth:

Sistemes de control de presencia, amb conversió Bluetooth-NFC
- Imma Pla (Dept. comercial) a Kimaldi: https://www.kimaldi.com
Línia de productes Suprema FaceStation / Biolite

Sistemes de diagnòstic de laboratori:

- José Luis Álvarez (Director dept. software comercial) Menarini Diagnóstics: https://www.menarinidiag.es/es-es/
Mesuradors de glucosa portàtils GlucoMen

- Jordi Pastor (IT Manager) Systelab Technologies (Werfen Clinical Software): https://www.werfen.com
No es fa servir la tecnologia Bluetooth. Els equips es connecten via Ethernet / USB / RS232

7. Annexos

7.1. Instal·lació sistema de virtualització Oracle Virtual Box

Per aquest treball s'ha utilitzat una màquina virtual sota el sistema de virtualització Oracle VirtualBox. S'ha triat aquest sistema atès que ja s'ha utilitzat i experimentat anteriorment en altres assignatures i disposar ja d'un equip físic ja configurat.

En aquest cas, per qüestions d'estabilitat s'ha fet servir la versió 6.1.40, en lloc de la més recent 7.0 disponible en el moment d'efectuar aquest treball Es pot descarregar des de el lloc web de Virtualbox.org:

https://download.virtualbox.org/virtualbox/6.1.40/VirtualBox-6.1.40-154048-Win.exe

> Nota: atès que la instal·lació de VirtualBox no aporta més informació rellevant, s'obvia la fase de instal·lació.

7.2. Configuració entorn auditor (Kali Linux)

Per aquest treball, s'ha utilitzat la distribució de seguretat Kali Linux[15] 2022.3 Aquesta distribució basada en Debian, es una derivació actualitzada de la distribució BackTrace utilitzada a la assignatura Seguretat de Xarxes de Computadors.

Per qüestions de temps, minimitzar configuracions de l'entorn, poder capturar i importar les dades més fàcilment, s'ha utilitzat una maquina virtual preconfigurada (disc virtual) de Kali preparada per a VirtualBox:

https://www.kali.org/get-kali/#kali-virtual-machines

Enllaç de descarrega: https://kali.download/virtual-images/kali-2022.3/kali-linux-2022.3-virtualbox-amd64.7z

Aquesta descarrega conté dos fitxers: amb la definició de la màquina virtual (fitxer .vbox) i el disc dur que conté el sistema operatiu ja preconfigurat (fitxer .vdi)

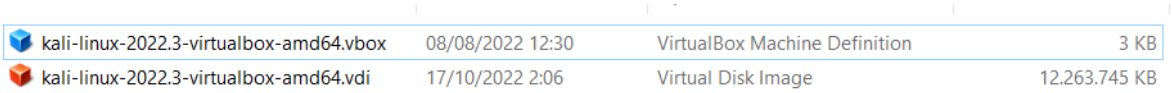

Figura 1: composició maquina virtual Kali Linux preconfigurada

15 Dades, informació i manuals d'ús a la web oficial Kali Linux: www.kali.org

En aquest cas, la instal·lació de la màquina virtual es simplifica, ja que només caldrà afegir la nova màquina des de el menú principal, pestanya *Máquina → Añadir* i triar el fitxer *kali-linux-2022.3-virtualbox-amd64.vbox*

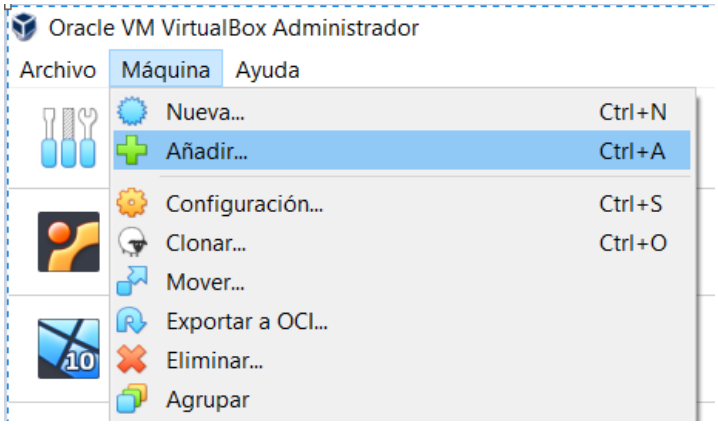

Figura 2: Importació maquina virtual

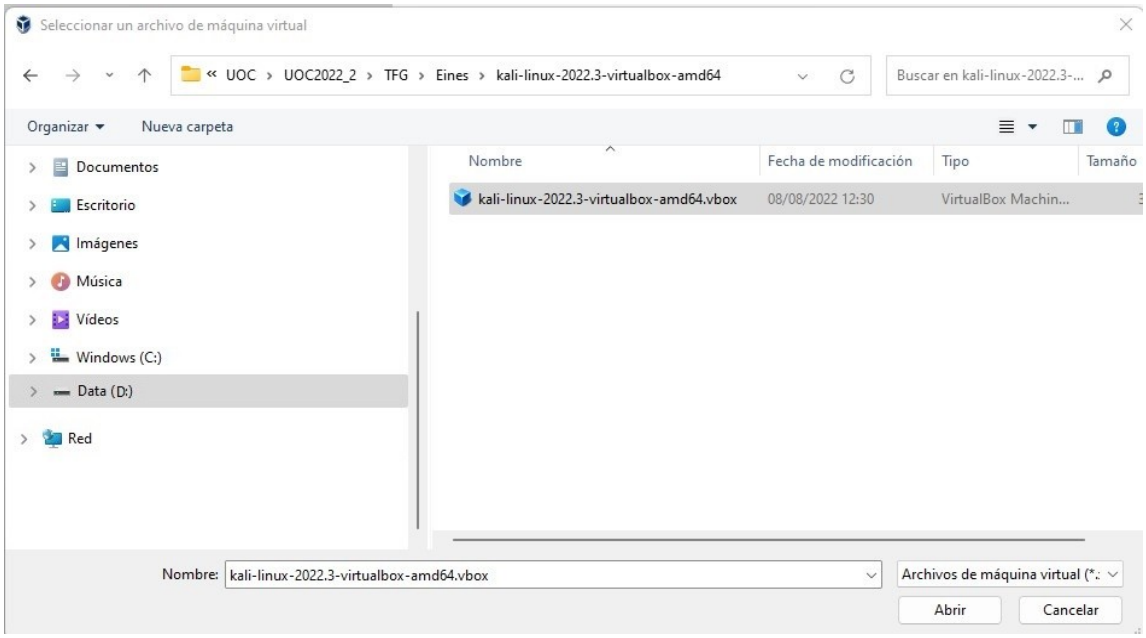

Figura 3: Importació maquina virtual. Carrega de l'arxiu de configuració

Si el fitxer es correcte, es mostrarà la configuració final preparada per a funcionar. En aquest cas, atès que l'equip amfitrió té prou memòria, es va modificar la quantitat de RAM fins a 4Gb per millorar el rendiment i minimitzar l'ús del disc dur (SSD) per a *swap*.

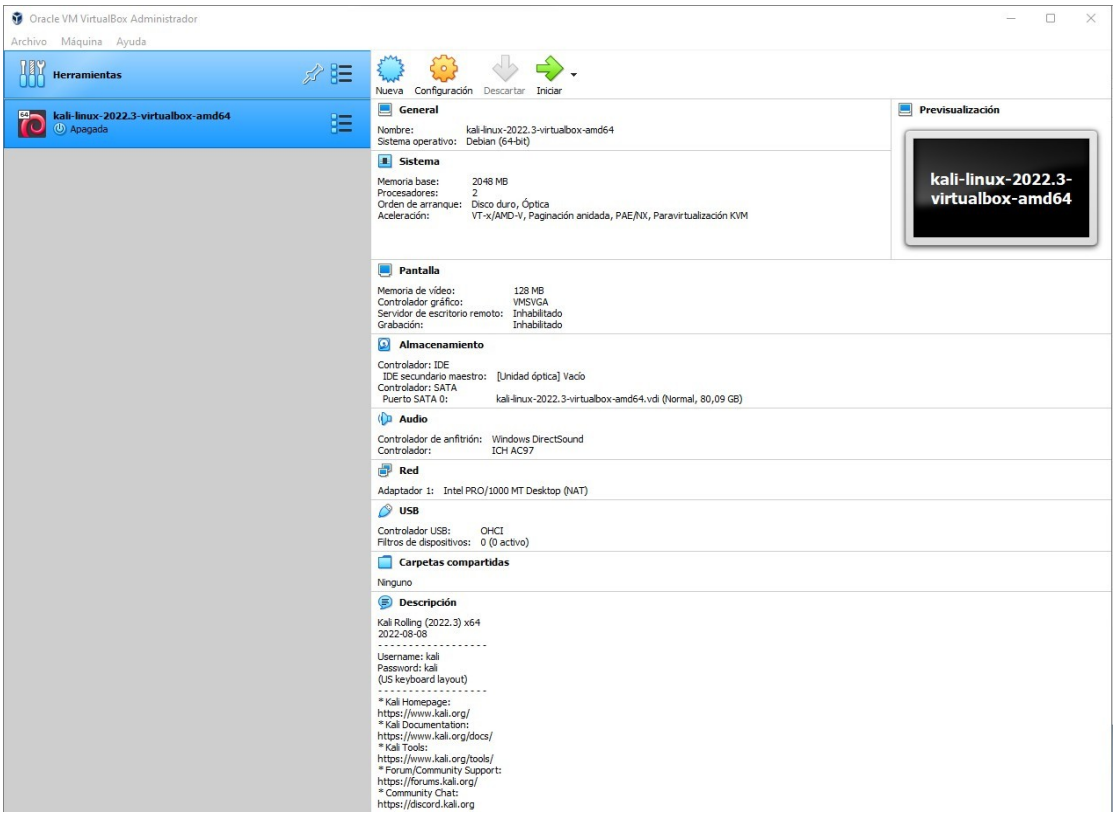

Figura 4: Importació maquina virtual. Configuració maquina importada.

Finalitzant la configuració del maquinari virtual, encenem el nou equip virtual. En encegar-se, es mostra les opcions d'inici del sistema. Si no es detecta cap pulsació del teclat, s'inicia automàticament amb KALI GNU/Linux després de 5 segons:

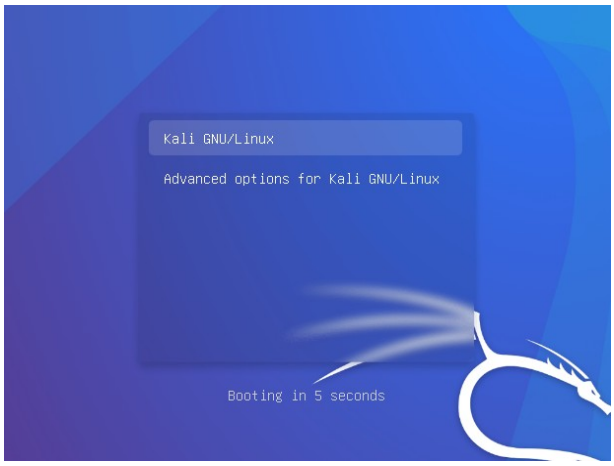

Figura 5: Pantalla inicial Kali Linux 2022.3

Pantalla inicial amb el login d'usuari de Kali Linux. Per defecte, l'usuari i la contrasenya es *kali*

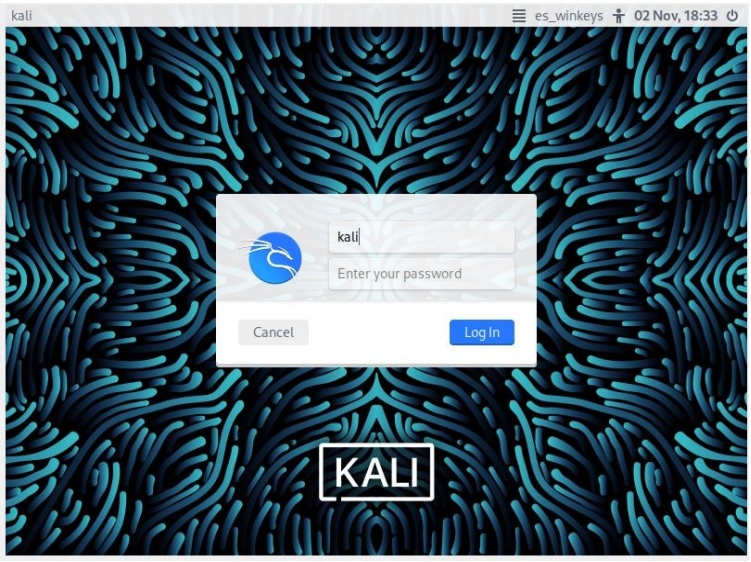

Figura 6: Pantalla inicial Kali Linux 2022.3. Login usuari

Al validar l'usuari, el sistema s'inicia mostrant l'escriptori:

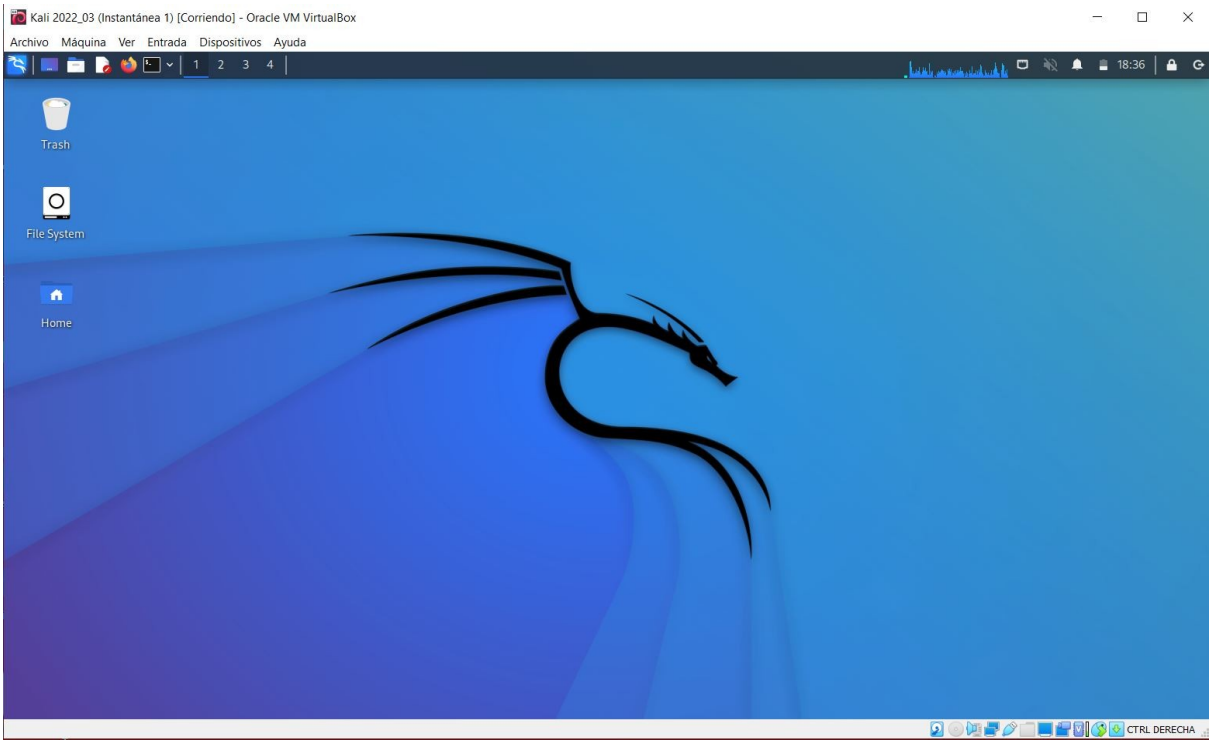

Figura 7: escriptori Kali Linux 2022.3

Amb el sistema ja iniciat, s'actualitza el sistema amb les últimes versions dels paquets i aplicacions. Es fa servir les comandes *sudo apt update* i *sudo apt-get update*

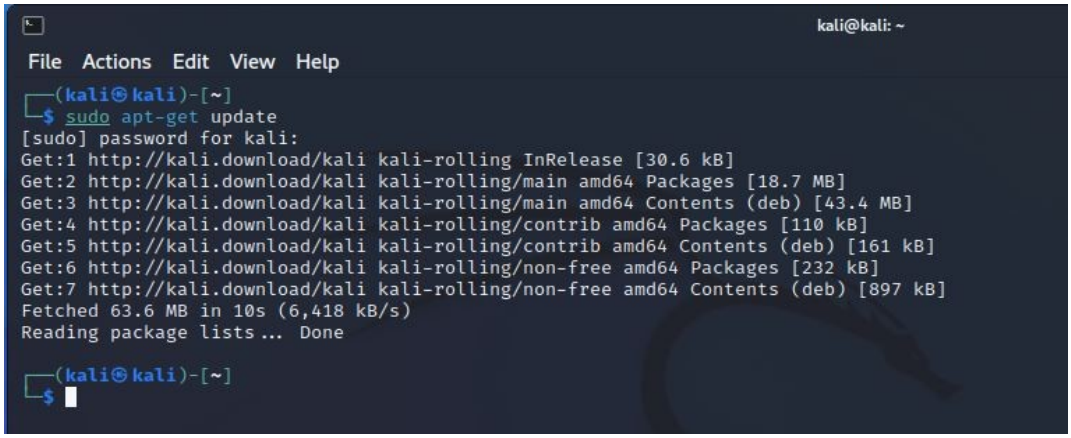

Figura 8: Actualitzant Kali

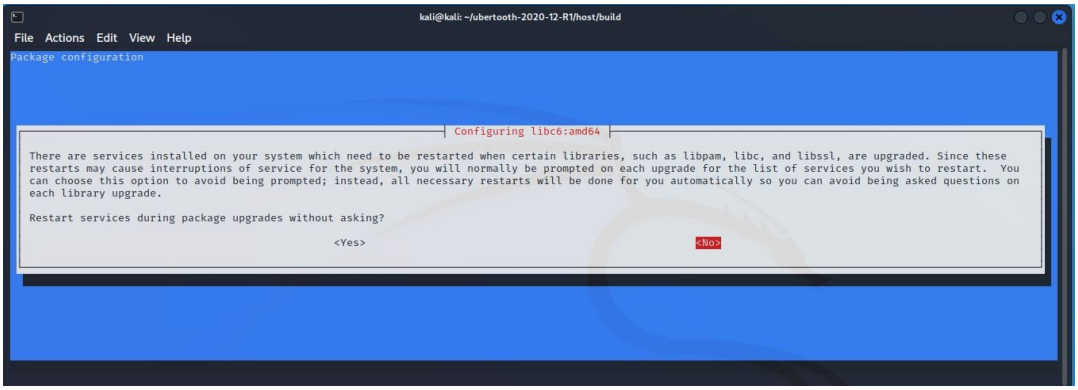

Figura 9: Actualitzant Kali. Serveis

Instal·lació del paquet de VirtualBox *Guest Additions* per poder gestionar correctament el dispositiu USB Bluetooth, millorar el suport del maquinari (USB, tarja gràfica) i la integració del ratolí/teclat/pantalla entre la màquina virtual i la física.

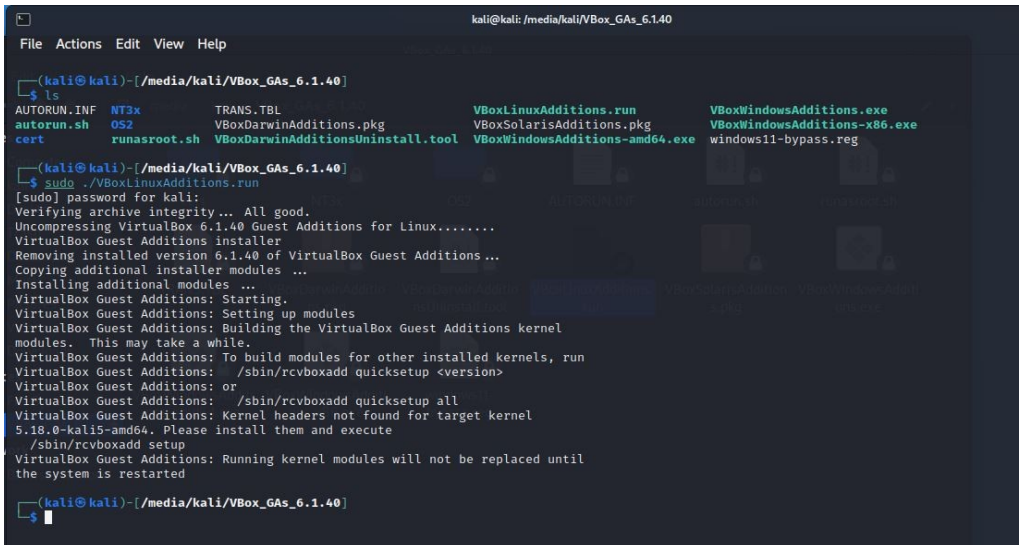

Figura 10: Instal·lació Virtual Box Guest Additions

7.3. Configuració entorn auditor maquinari (Ubertooth)

En aquest treball, s'ha utilitzat una sonda USB Bluetooth Ubertooth One[16] del fabricant Great Scott Gadgets[17] . Aquest dispositiu es un desenvolupament OpenSource de Michael Ossmann[18](CEO de Great Scott Gadgets) i Dominic Spill, orientat a experimentar amb la connectivitat, captura i injecció de tràfic amb Bluetooth BLE i clàssic (BR).

Integra un processador ARM i un petit amplificador de senyal. S'alimenta directament de la connexió USB 2.0 de l'equip.

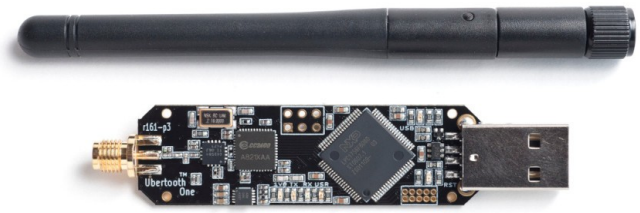

Figura 11: Sonda Ubertooth One
Origen imatge: https://greatscottgadgets.com/images/ubertooth-and-antenna.jpeg

Té dues funcions:

- Permet millorar la amplada de recerca dels dispositius Bluetooth.
- Testejar amb més precisió els dispositius a analitzar.

Com a mesura de seguretat i prevenir un ús inadequat, el fabricant implementa un límit a la quantitat de paquets (payload) que pot enviar cap a un dispositiu per testejar.

De la mateixa forma que Kali Linux, l'ús d'aquesta eina es exclusivament per fer una anàlisi o auditoria de seguretat dels dispositius. En cap cas, no es farà servir juntament amb altres eines de Kali, per obtenir informació d'altres equips que no participen a la prova.

La configuració del dispositiu consta de dues parts:

- Instal·lació del programari i utilitats.
- Actualització del firmware del dispositiu.

16 https://greatscottgadgets.com/ubertoothone/
17 Web del fabricant https://greatscottgadgets.com/
18 Llicència OpenSource: https://ubertooth.sourceforge.net/

7.3.1. Instal·lació del programari i utilitats

Previ a la instal·lació, es necessari configurar VirtualBox per que el dispositiu USB que està connectat a la maquina física, pugui ser detectat per la màquina virtual. La figura mostra el procediment i la ruta:

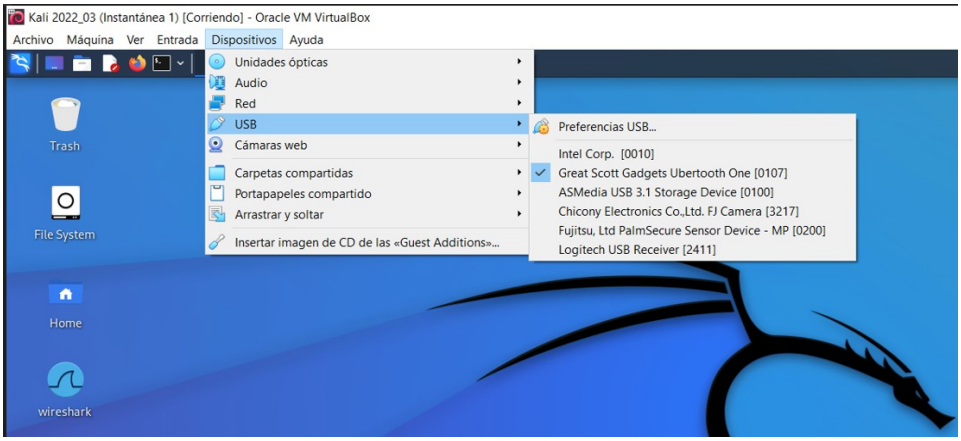

Figura 12: Configuració USB Ubertooth One

Seguint la guia del fabricant [19] pas a pas, s'instal·len i compilen les llibreries de suport Bluetooth libusb:

```
sudo apt-get install git cmake libusb-1.0-0-dev make gcc g++ libbluetooth-
dev \ pkg-config libpcap-dev python-numpy python-pyside python-qt4
```

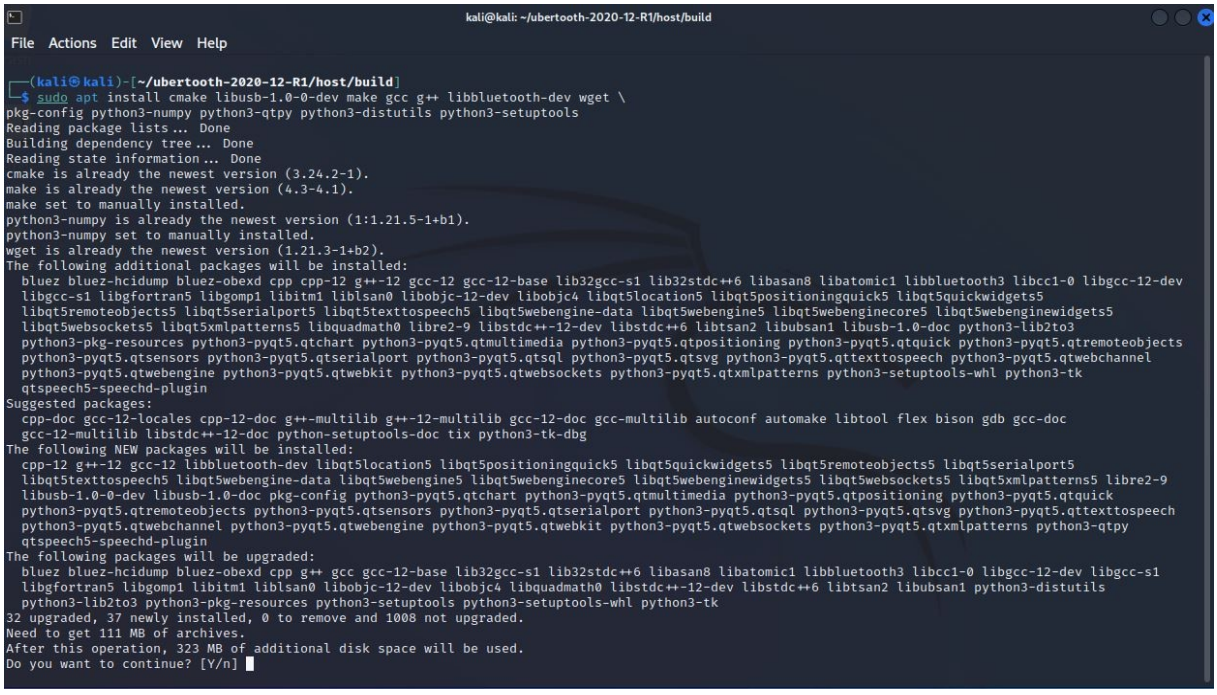

Figura 13: Actualització llibreries libbusb

19 Guia d'instal·lació i configuració: https://ubertooth.readthedocs.io/en/latest/build_guide.html

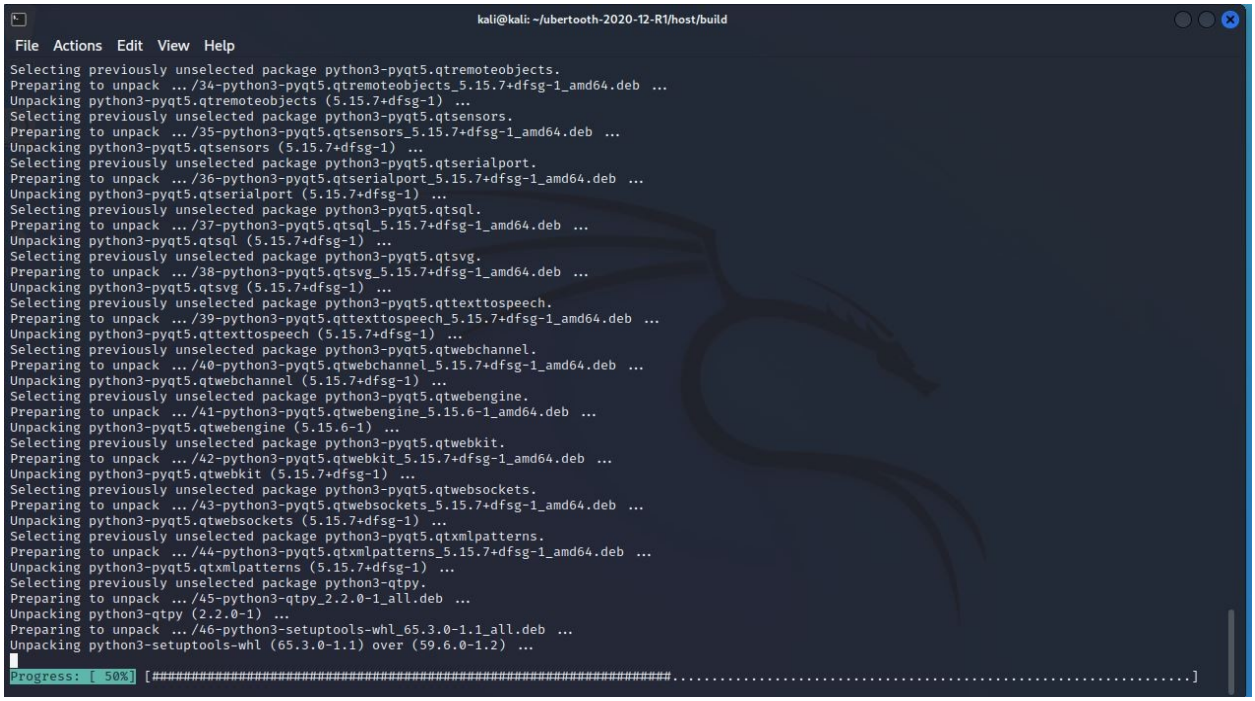

Figura 14: Actualització llibreries libusb (2)

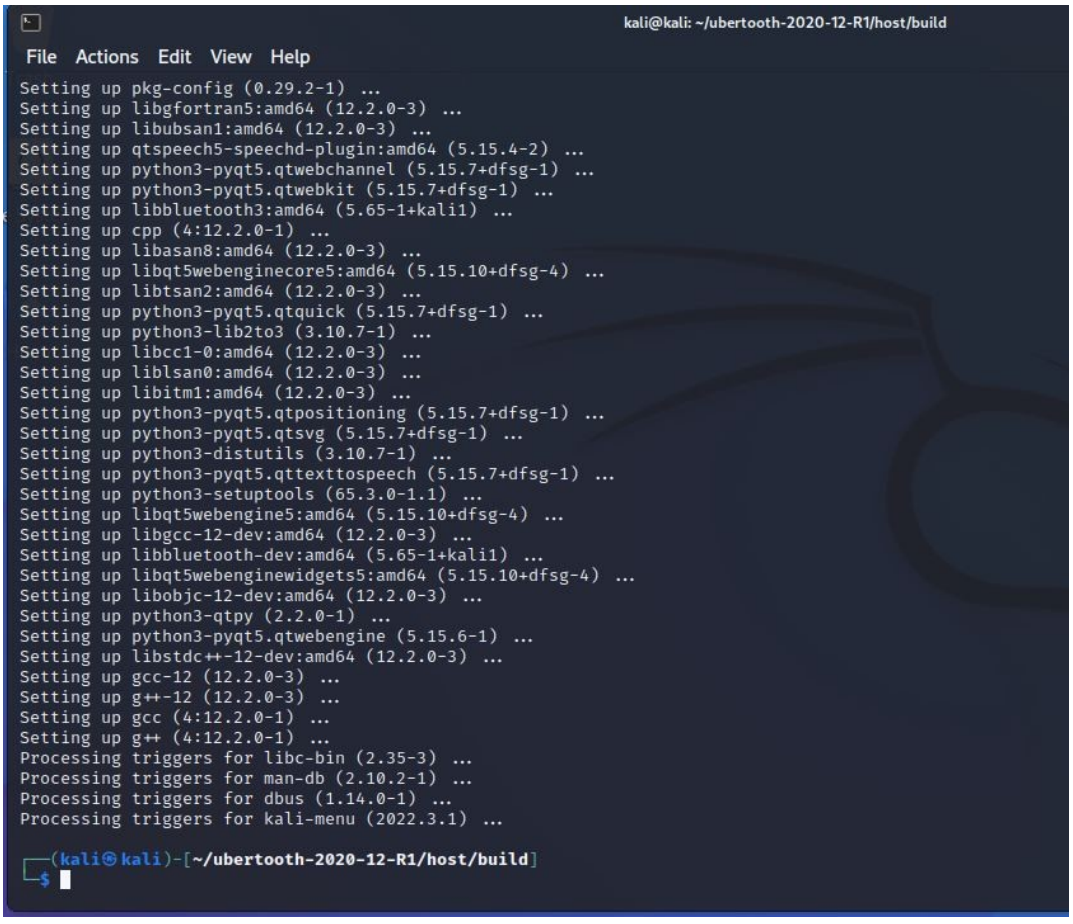

Figura 15: actualització llibreries libbusb (3)

Amb el paquet actualitzat, es descarrega la llibreria libbtbb del repositori de GitHub del fabricant, per suport i anàlisi millorat dels paquets Bluetooth i creació del set up posterior amb les comandes make i cmake:

```
wget https://github.com/greatscottgadgets/libbtbb/archive/2020-12-
R1.tar.gz -O libbtbb-2020-12-R1.tar.gz
tar -xf libbtbb-2020-12-R1.tar.gz
cd libbtbb-2020-12-R1
mkdir build
cd build
cmake ..
make
sudo make install
sudo ldconfig
```

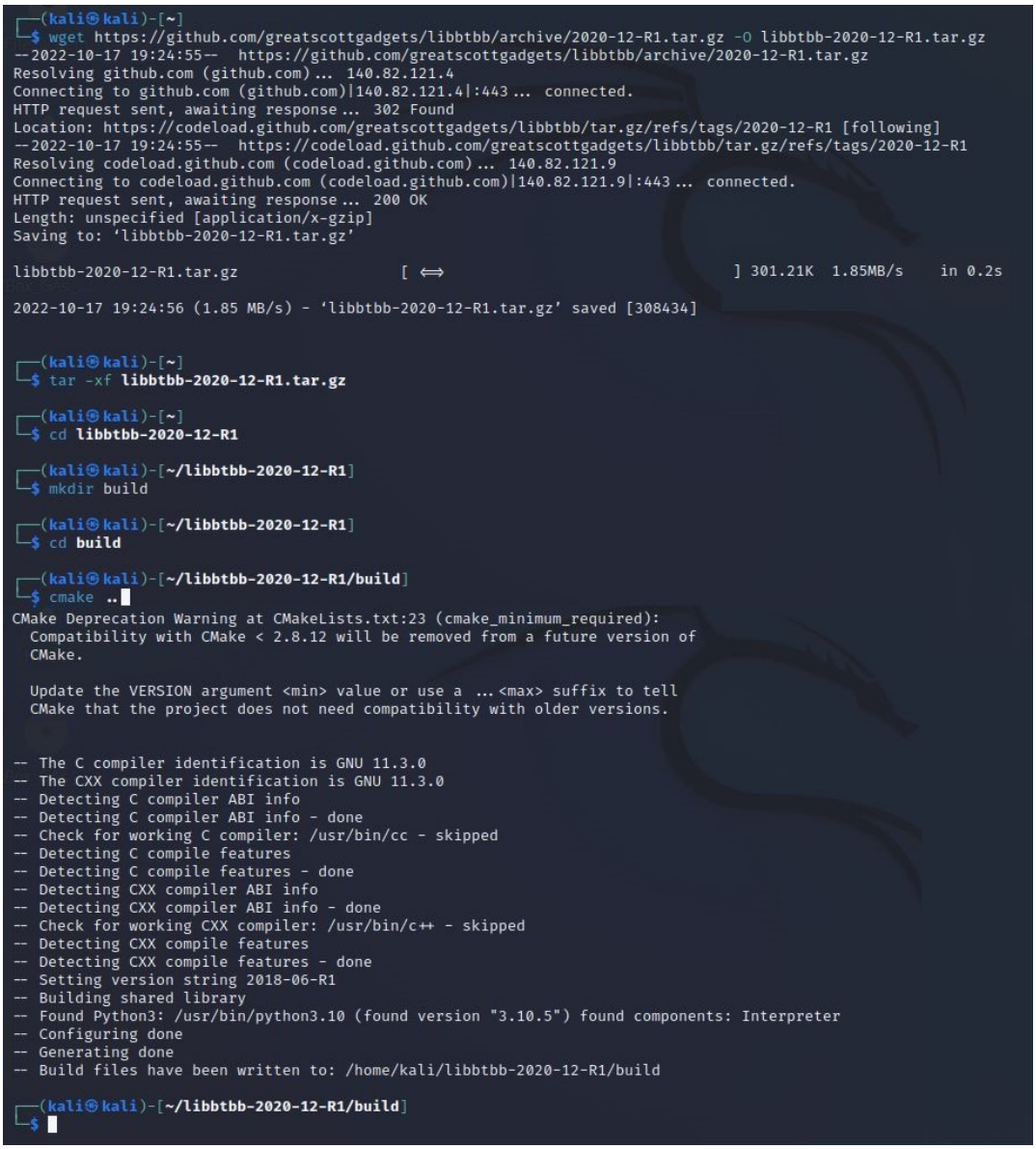

Figura 16: Instal·lació llibreria libbtbb. Cmake

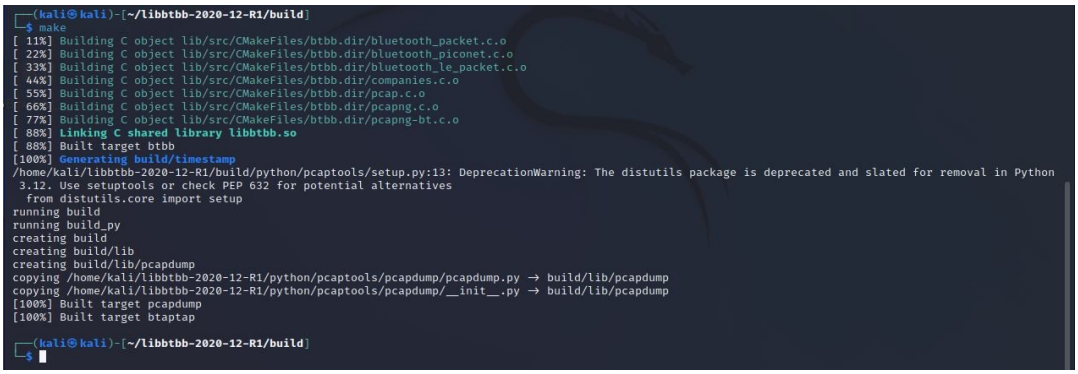

Figura 17: Instal·lació llibreria libbtbb . Make

Figura 18: Instal·lació llibreria libbtbb. Finalització

7.3.2. Instal·lació de les eines Ubertooth tools

Aquest paquet conté les eines per a capturar els paquets i actualitzar el firmware del dispositiu. S'instal·len amb aquesta seqüència de comandes:

```
wget https://github.com/greatscottgadgets/ubertooth/releases/download/2020-12-R1/
ubertooth-2020-12-R1.tar.xz

tar -xf ubertooth-2020-12-R1.tar.xz
cd ubertooth-2020-12-R1/host
mkdir build
cd build
cmake ..
make
sudo make install
sudo ldconfig
```

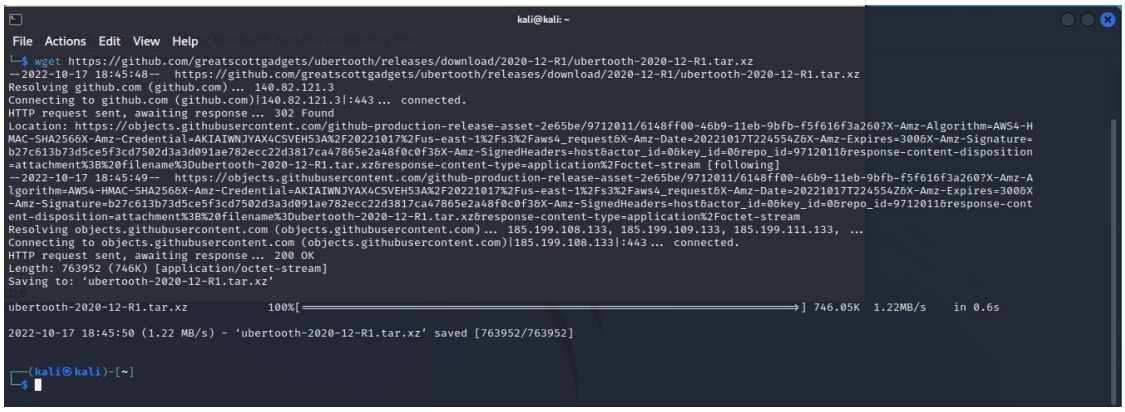

Figura 19: Instal·lació Ubertooth tools

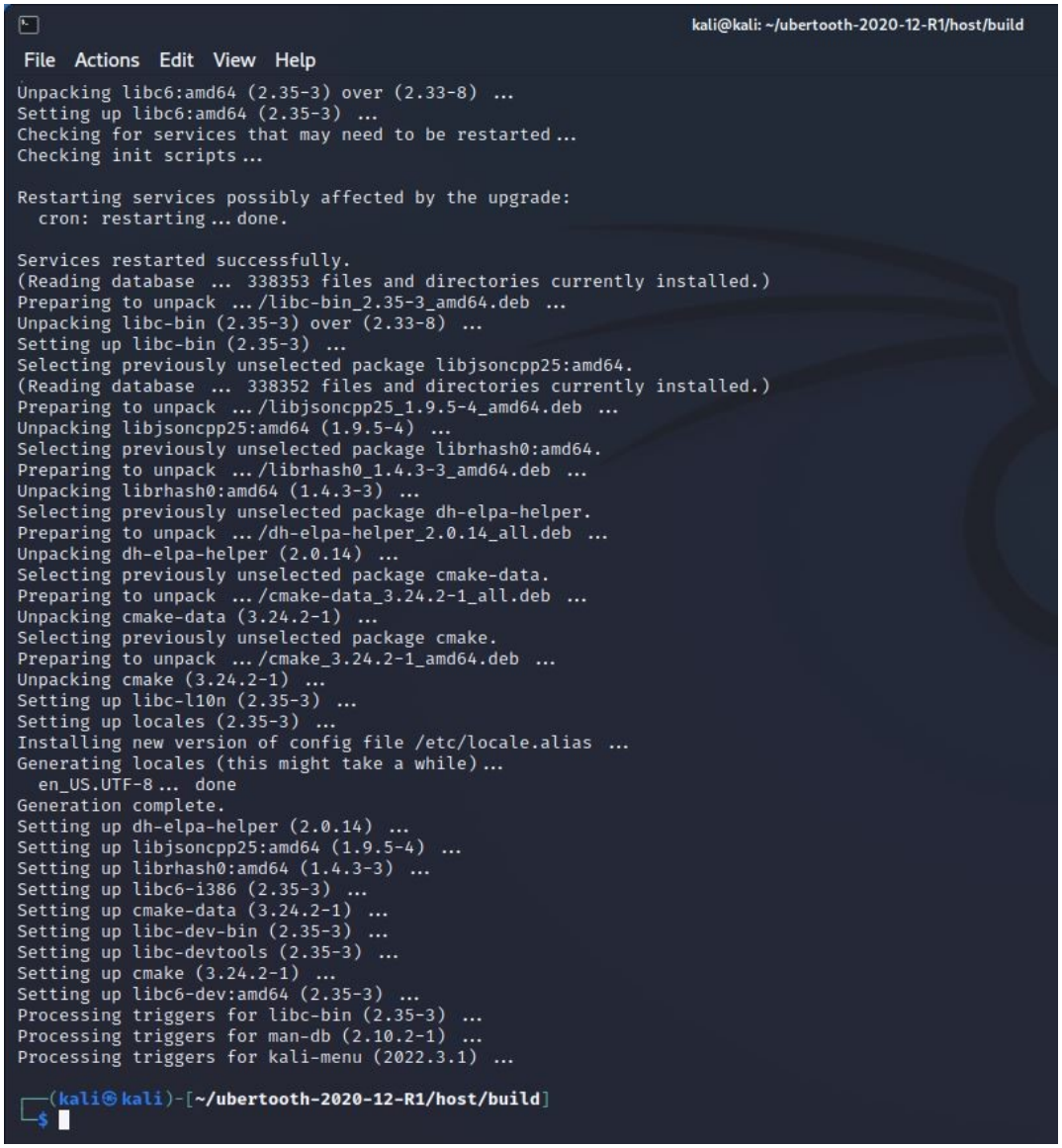

Figura 20: Instal·lació Ubertooth tools. Cmake/make

7.3.3. Actualització del firmware del dispositiu Ubertooth One

Comprovació de la versió actual que porta el dispositiu amb les comandes:
`ubertooth-util -v` (mostra la versió)
`ubertooth-util -V` (mostra la versió, autor i data)

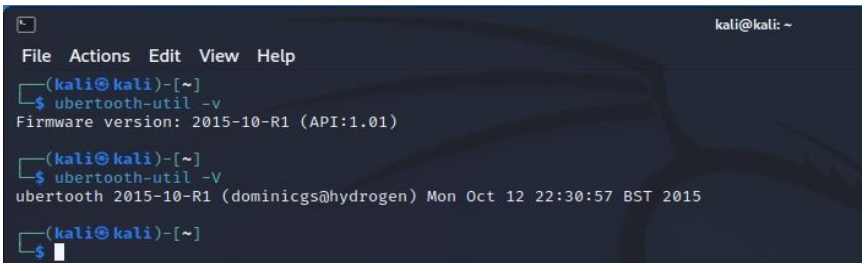

Figura 21: Informació versió firmware instal·lat

La descarrega de les eines Ubertooh inclou la versió més actual i estable del firmware. En aquest cas, 2020-12-R1

Per actualitzar el dispositiu, es fa servir la comanda:

```
ubertooth-dfu -d bluetooth_rxtx.dfu -r
```

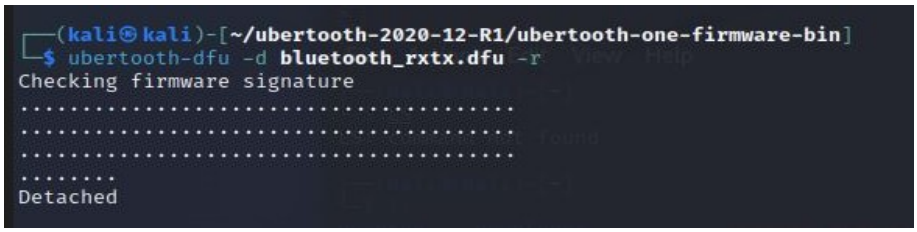

Figura 22: Instal·lació firmware

Verificació del dispositiu actualitzat:

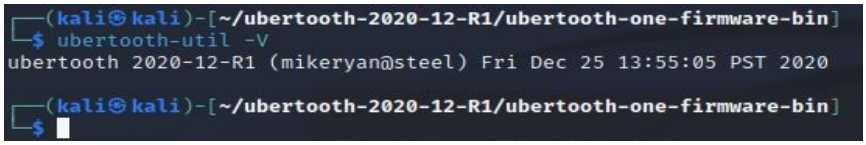

Figura 23: Verificació versió firmware actualitzat

7.3.4 Comprovació funcionament dispositiu

Des de Wireshark. En aquest cas, es requereix crear un canal (pipe) amb la comanda `mkfifo /tmp/pipe` i triar aquesta connexió des de Wireshark:

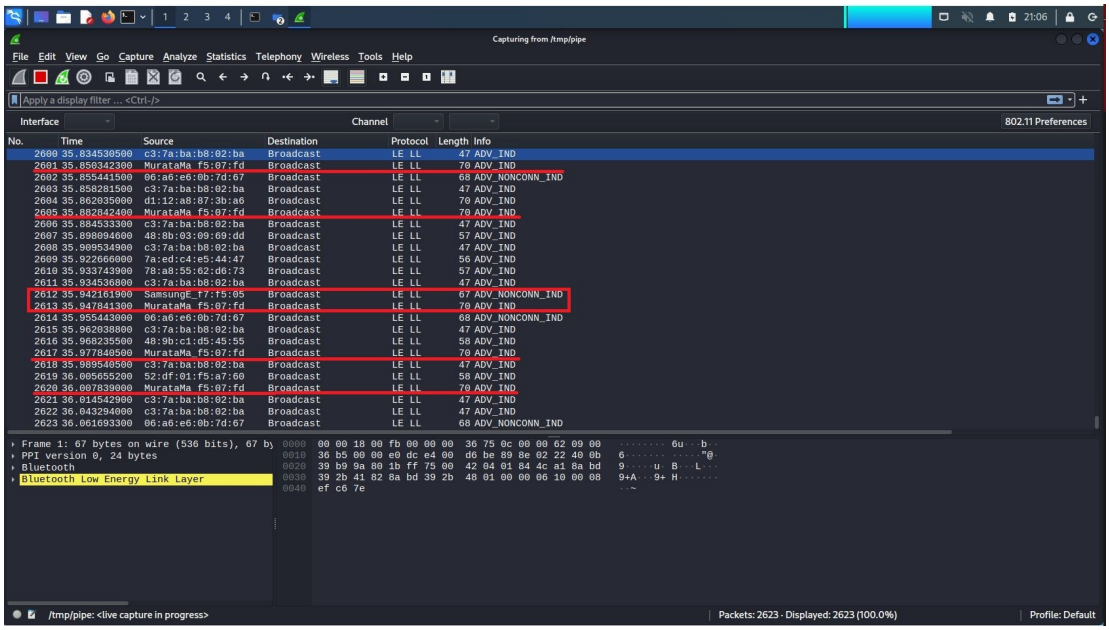

Figura 24: captura dades des de Wireshark

Des de terminal, amb la comanda `ubertooth-btle -f -c /tmp/pipe`

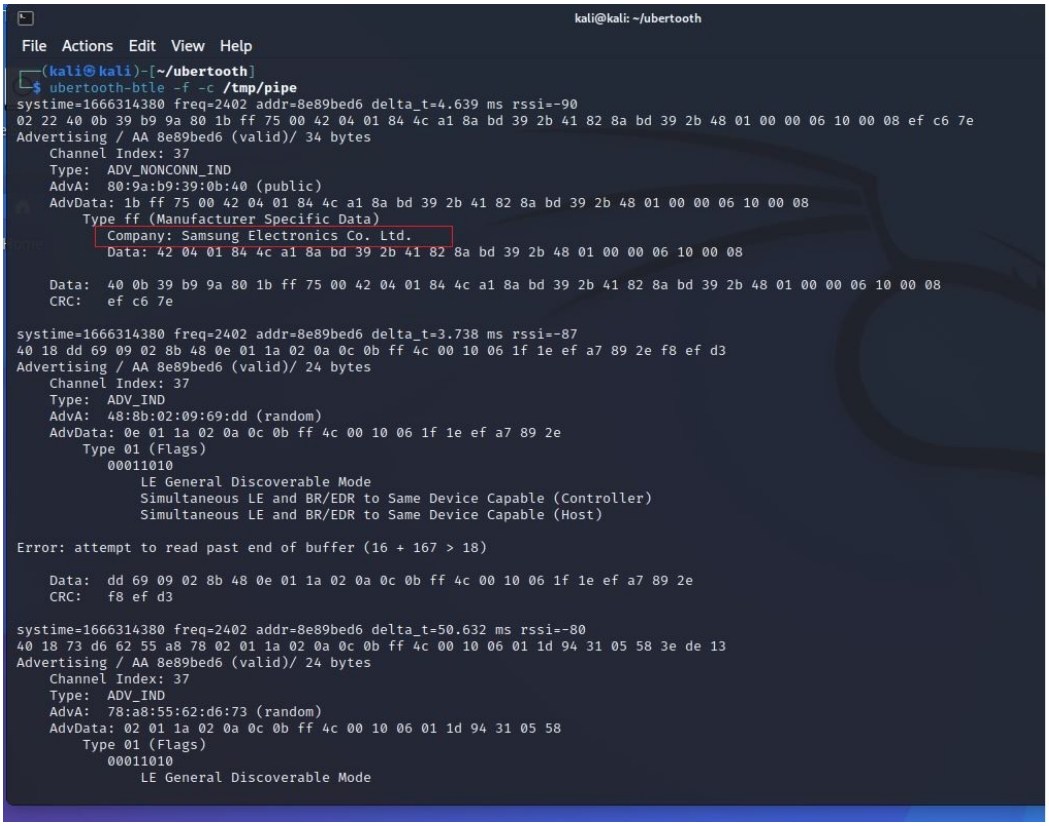

Figura 25: Captura dades amb Ubertool

En totes dues captures subratllat en vermell, podem comprovar que es mostren dades de dispositius, Bluetooth BLE (Samsung, Murata).
També podem fer servir el dispositiu Ubertooth One com analitzador d'espectre del rang de freqüències de Bluetooth (2,400 ~ 2,480Ghz), amb la comanda `ubertooth-specan-ui`

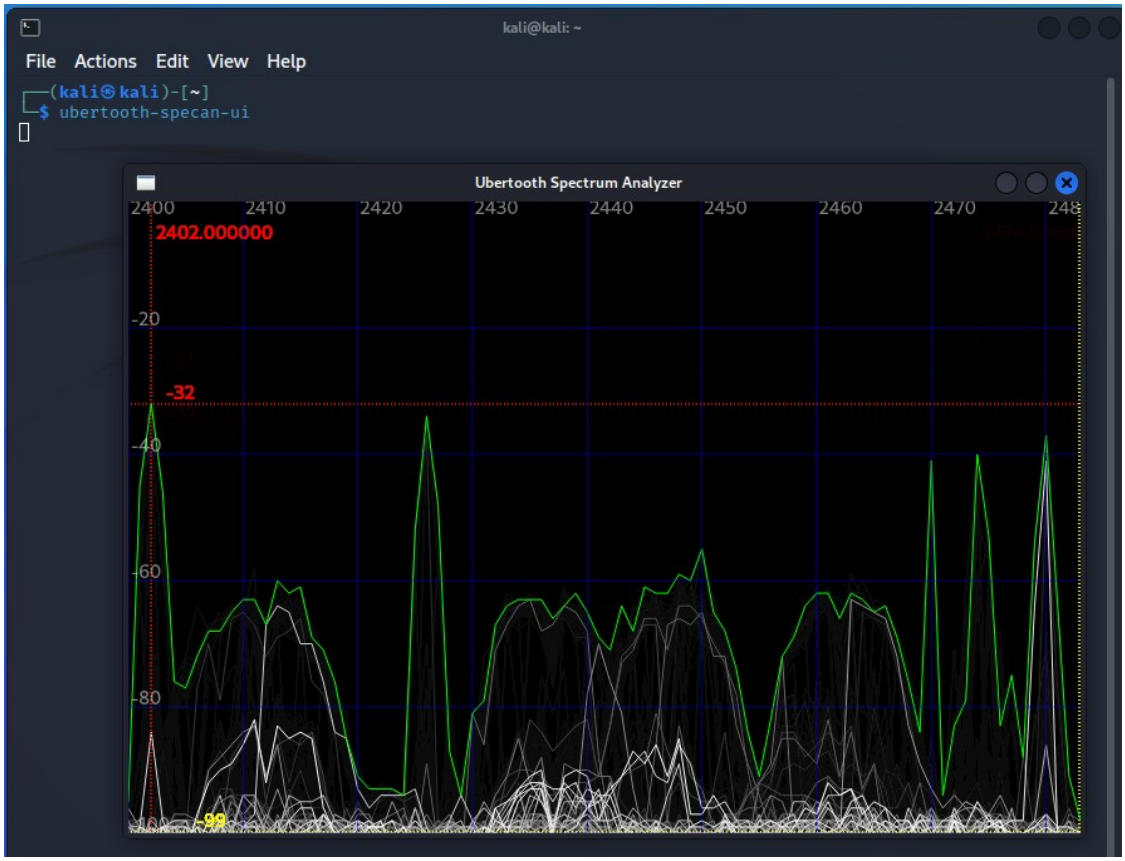

Figura 26: Anàlisi de l'espectre