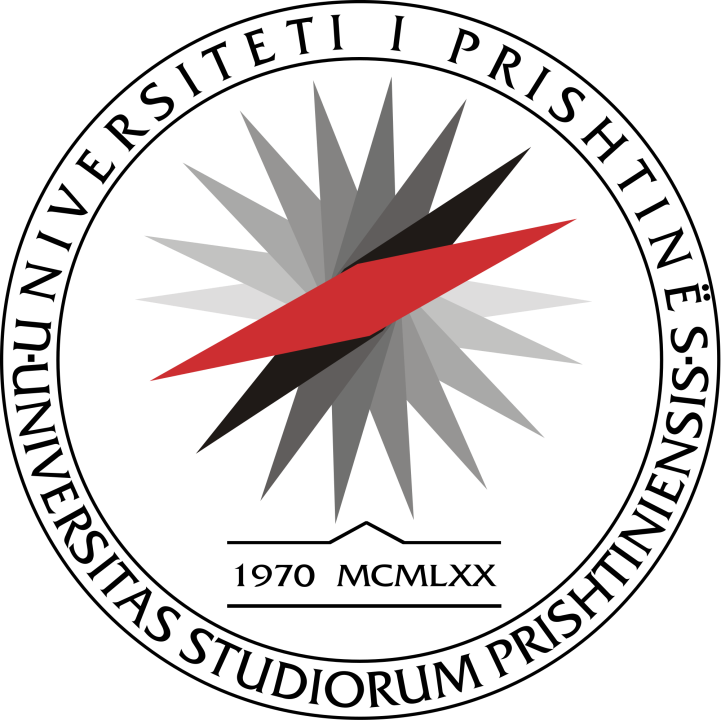
**UNIVERSITETI I PRISHTINËS "HASAN PRISHTINA"**

FAKULTETI I INXHINIERISË ELEKTRIKE DHE KOMPJUTERIKE

DEPARTAMENTI I INXHINIERISË KOMPJUTERIKE  
STUDIMET MASTER



Raport: “Analiza e veglës Kismet ”  
 Lënda: “Sigurimi i informacionit”

Profesor: Prof. Dr. Blerim Rexha Studentët:

Leontina Hulaj

Visar Berisha

Lundrim Rexhepi

Prishtinë, 2020

Contents

[Hyrje 3](#_Toc59569386)

[Kismet 3](#_Toc59569387)

[Komponentët e Kismet 3](#_Toc59569388)

[Karakteristikat e Kismet 3](#_Toc59569389)

[Përdorimi I Kismet 4](#_Toc59569390)

[Përfundim 10](#_Toc59569391)

# Hyrje

Pajisja Wi-Fi është shumë e ndjeshme ndaj piraterisë sepse sinjalet e krijuara nga një pajisje Wi-Fi mund të zbulohen nga çdokush. Shumë rutera përmbajnë dobësi që mund të shfrytëzohen me mjete softuerësh të pranishëm në sistemin operativ Kali Linux.

ISP-të dhe Router-i kanë të aktivizuar sigurinë WPS të parazgjedhur që i bën këto pajisje të prirura ndaj sulmeve wireless. Kjo e bën sigurinë per wireless një gjë thelbësore.

Nje nga mjetet kryesore per sulme wireless eshte eshte paketa Kismet.

# Kismet

Kismet është një open source 802.11 detektor dhe analizues i rrjetit wireless, sistem i zbulimit ndërhyrjeve. Funksionon me çdo kartë wireless që mbështet modalitetin e monitorimit të papërpunuar (rfmon) dhe mund të nuhasë trafikun 802.11a / b / g / n.

Kismet është jashtëzakonisht i konfigurueshëm. Mund të konfigurohet për të kërcyer nëpër të gjitha kanalet dhe për të analizuar të gjithë rrjetin wireless. Mund të konfigurohet në një mënyrë që të punojë vetëm për një kanal të dedikuar për të analizuar trafikun për një kanal të vetëm.

Ai identifikon rrjetin duke mbledhur pako në mënyrë pasive dhe zbulimin e rrjeteve të emërtuara, zbulimin e rrjeteve të fshehura përmes trafikut të të dhënave. Kjo është paketa kryesore që përmban berthamen(core), klientin dhe serverin.

Kismet eshte I disponueshem per Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

## Komponentët e Kismet

Kismet vjen me serverin Kismet (kismet\_server) dhe klientin Kismet (kismet\_client).

Serveri Kismet është ai që kryen nuhatjen(sniffing) e paketës dhe zbulimin e rrjetit, ndërsa klienti i Kismet është GUI. Nëse duhet bere ndonjë konfigurim shtesë, mund të modifikohet skedari Kismet.conf në / etc / kismet /.

## Karakteristikat e Kismet

Kismet ka aftësinë për të zbuluar rrjete, madje edhe rrjete që fshehin qëllimisht ekzistencën e tyre duke çaktivizuar transmetimin e SSID të tyre.

Këtë e bën me “channel-hopping", i cili është një proces i skanimit të secilit kanal në brezin e frekuencës 2.4 GHz.

Kismet është një ndegjues "pasiv", prandaj nevoja për modalitetin Monitor.

Duke identifikuar rrjetet, Kismet do të shfaq adresën e saj MAC (BSSID), SSID (emri i rrjetit), kanali në përdorim, llojin e kriptimit, numrin e paketave që transmetojnë në rrjet, të dhënat që u shfaqen në rrjet për herë të fundit, dhe madje edhe adresat MAC të klientëve të lidhur me një AP të veçantë.

## Përdorimi I Kismet

Kismet mund të përdoren për të identifikuar dhe për të audituar rrjetet wireless dhe konfigurimin e tyre.

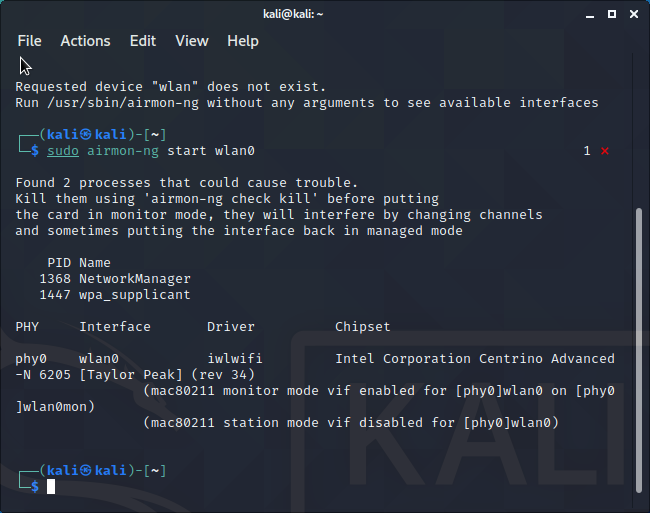
Ato gjithashtu mund të përdoren për të identifikuar rrjetet wireless që janë konfiguruar keq ose madje edhe kanë AP të paautorizuar.

Hakerat mund të përdorin Kismet për të identifikuar rrjetet e fshehura ose rrjetet që janë të ekspozuara për tu shfrytëzuar.

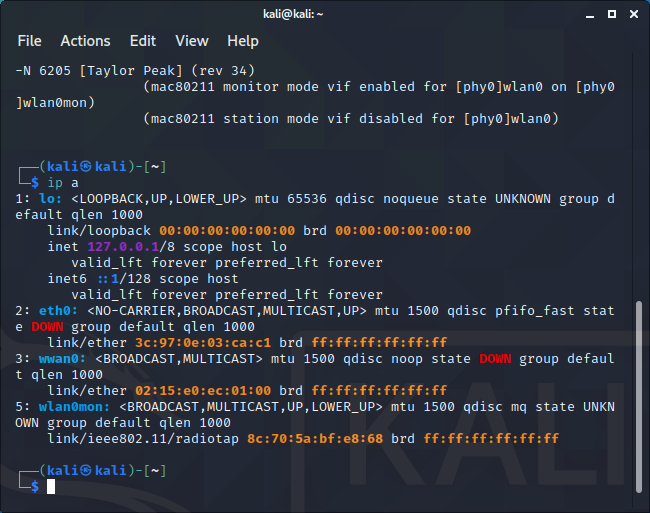
Ne vazhdim mund te shihni procesin për të parë aktivitetin e përdoruesit të Wi-Fi përmes mureve(walls).

Para se të fillojmë Kismet, duhet të shtojmë një burim pakete (packet source). Ky do të jetë adapteri wireless.

**Hapi 1.** Së pari hapet terminali dhe shtypet komanda “airmon-ng start wlan-0”. Kjo komandë mundëson kthimin e kartës wireless nga modaliteti I menaxhuar në modalitetin e monitorimit.

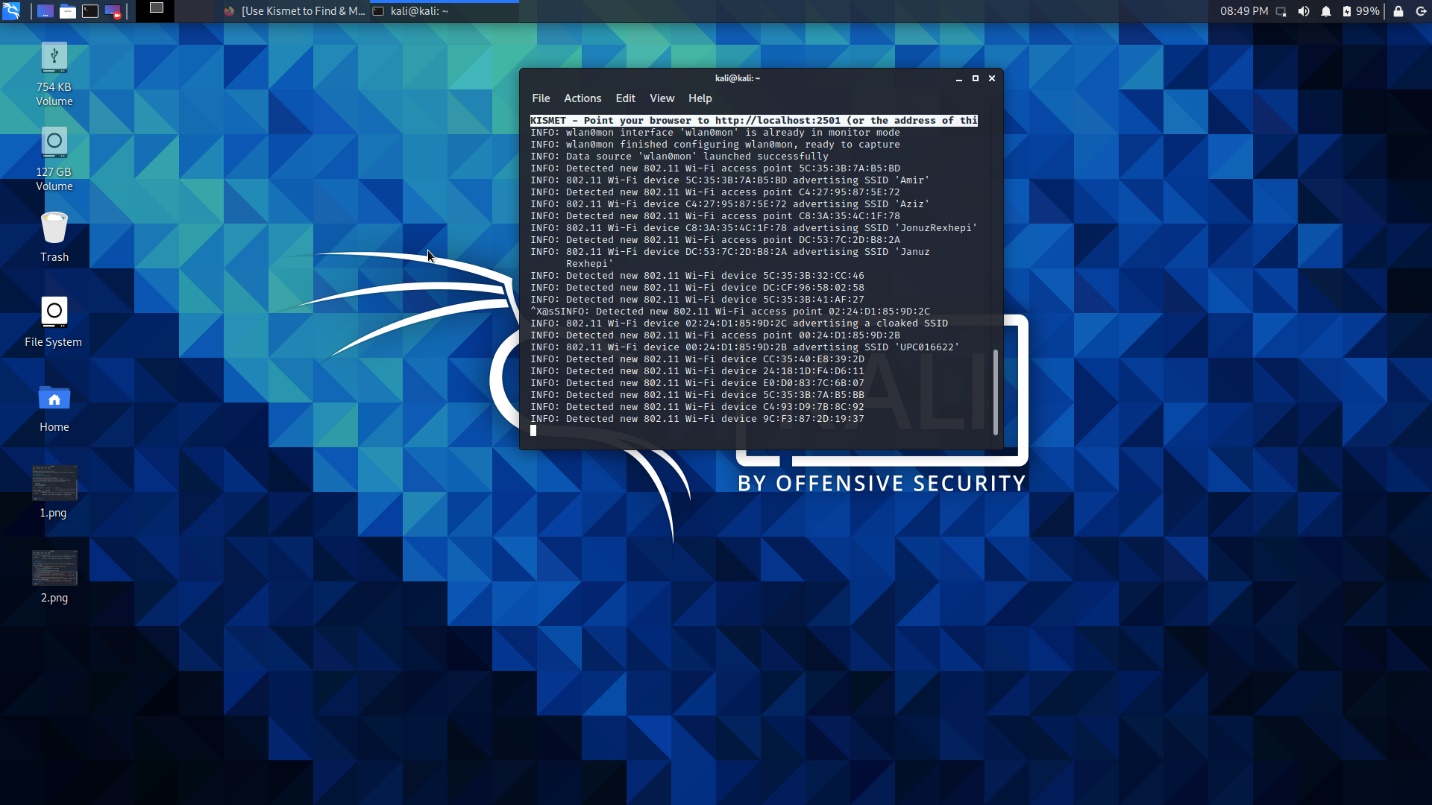


**Hapi 2.** Pastaj në terminal shkruaj komandën “ip a”. Komanda ip në Linux përdoret për kryerjen e disa detyrave të administrimit të rrjetit. IP qëndron për Protokollin e Internetit. Kjo komandë përdoret për të treguar ose manipuluar rutingun, pajisjet dhe tunelet, po ashtu edhe caktimin e një adrese në një ndërfaqe rrjeti ose konfigurimin e parametrave të ndërfaqes së rrjetit.



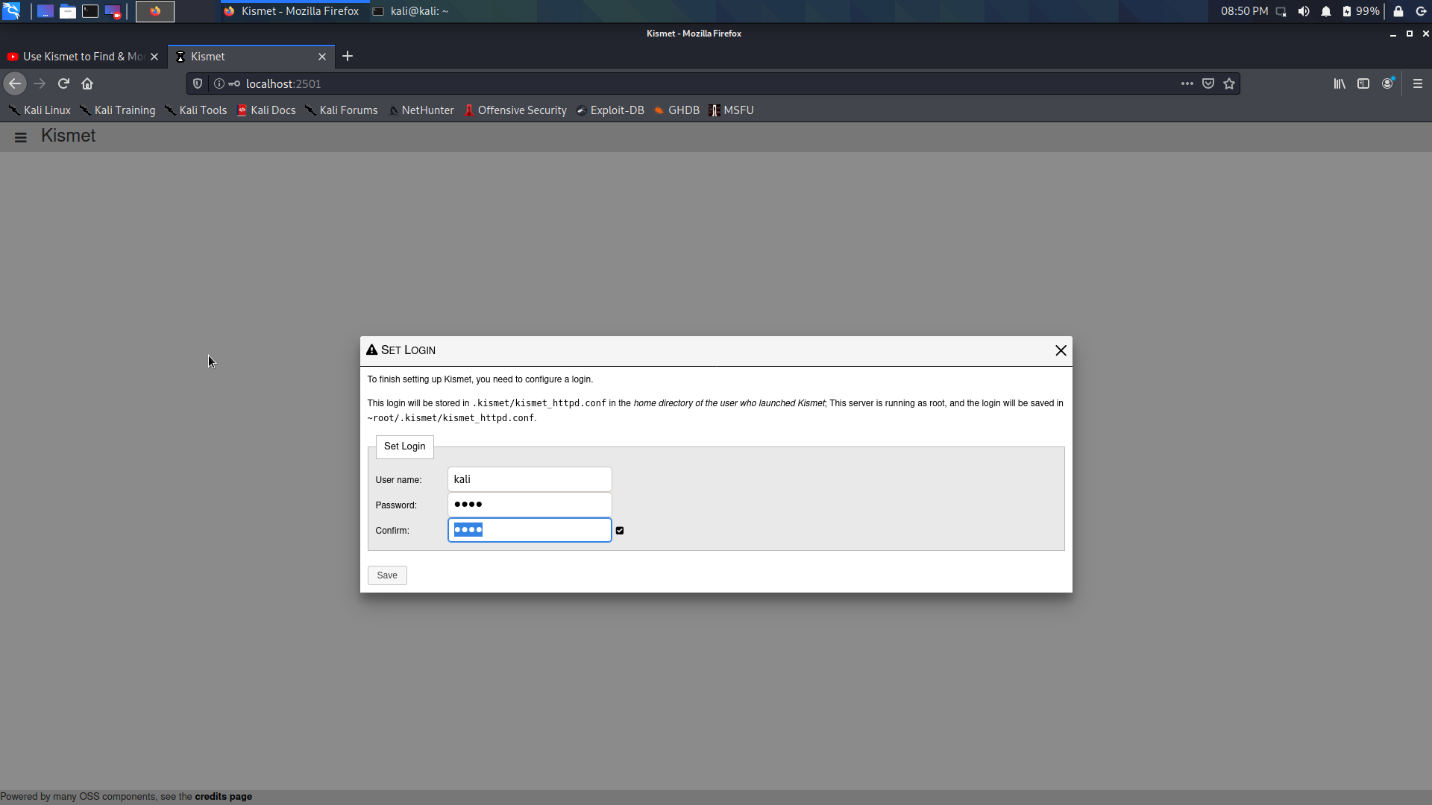
Kjo do të tregojë informacionin në lidhje me të gjitha ndërfaqet e disponueshme në sistemin tone.

**Hapi 3.** Për të lancuar serverin e Kismet shkruhet në terminal “kismet”.



Në fotografi shihet startimi I serverit Kismet. Nese klikohet linku http:://localhost:2501 do të hapet serveri në browser.

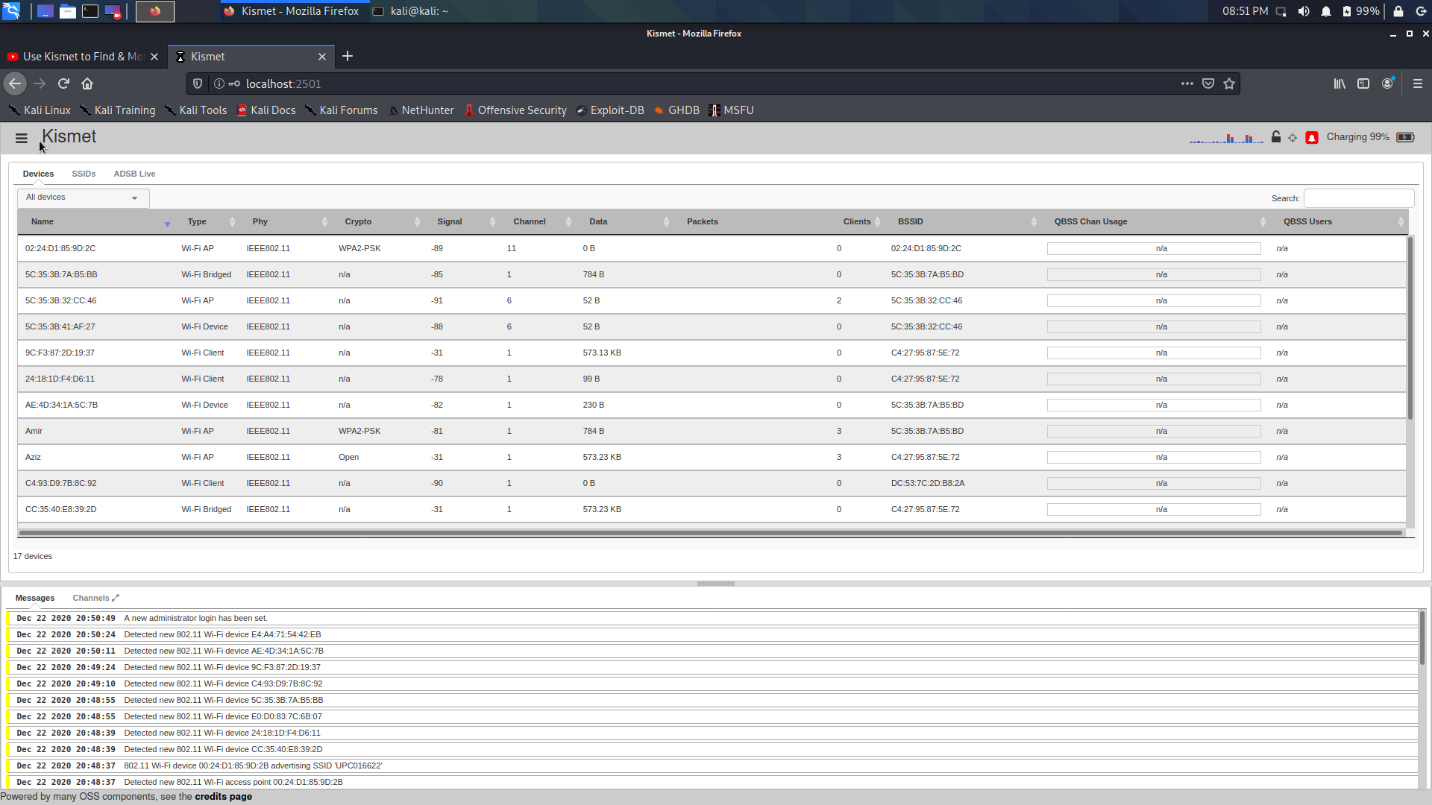
**Hapi 4.** Logini si administrator



Siq shihet edhe në fotografi për ta hapur në browser serverin kërkon konfirmimin e login si administrator duke dhënë emrin dhe paswordin e administruesit. Këto të dhëna ruhen në .kismet/kismet\_httpd.config.

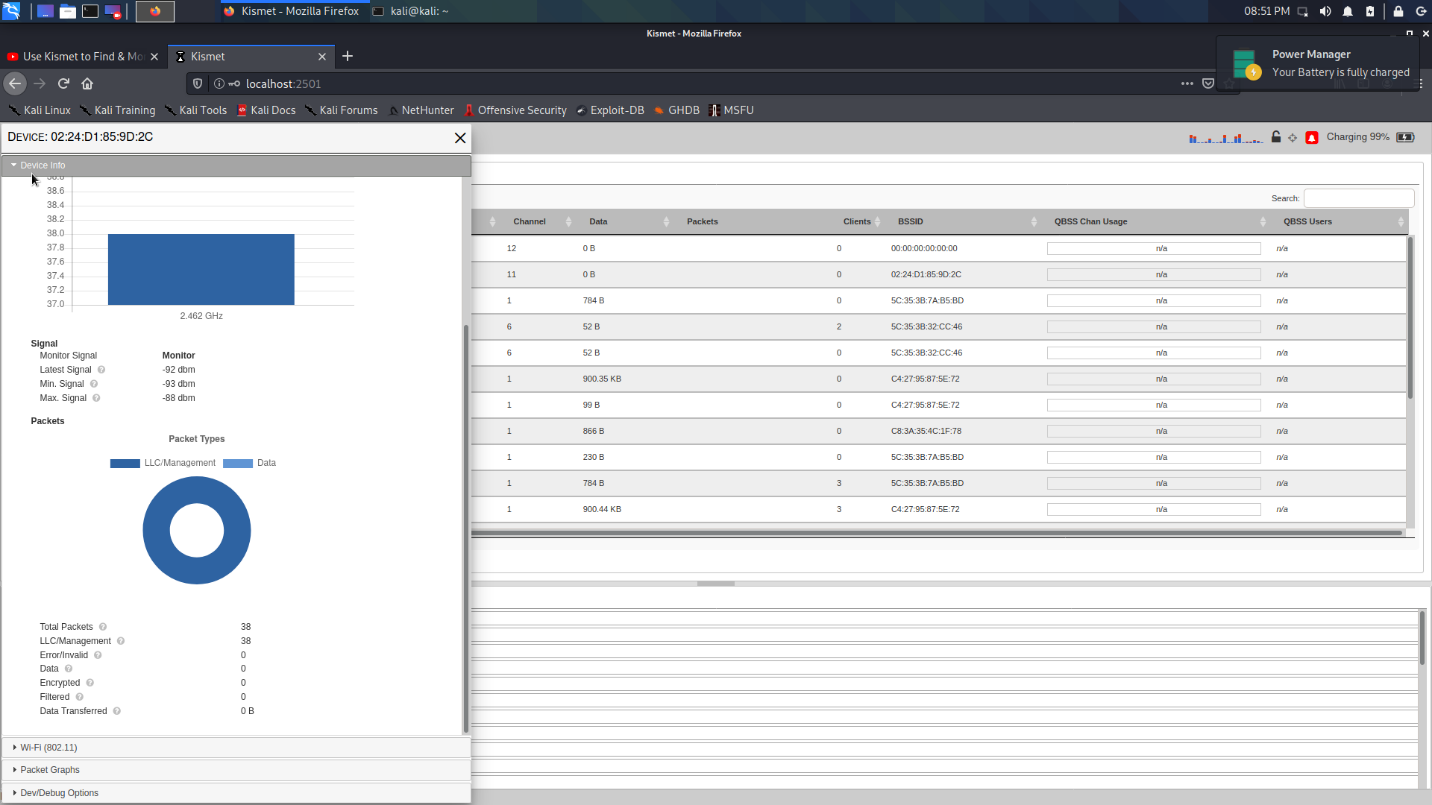
Kismet na lejon të shohim informacionin e mëposhtëm në lidhje me një rrjet të veçantë:

* SSID (emri i rrjetit)
* BSSID (adresa MAC e Access Point)
* Prodhuesi i AP
* Koha kur u pa për herë të parë rrjeti
* Koha kur u pa për herë të fundit rrjeti
* Mënyra e AP (ad hoc ose e Menaxhuar / Infrastruktura)
* Kanali në përdorim
* Frekuenca
* Reklamim ose SSID i fshehur
* Lloji i kriptimit (nëse ka)
* Fuqia e sinjalit
* Zhurma
* Paketat totale të kapura
* Paketat totale të të dhënave te kapura
* Paketat totale të menaxhimit të kapura.

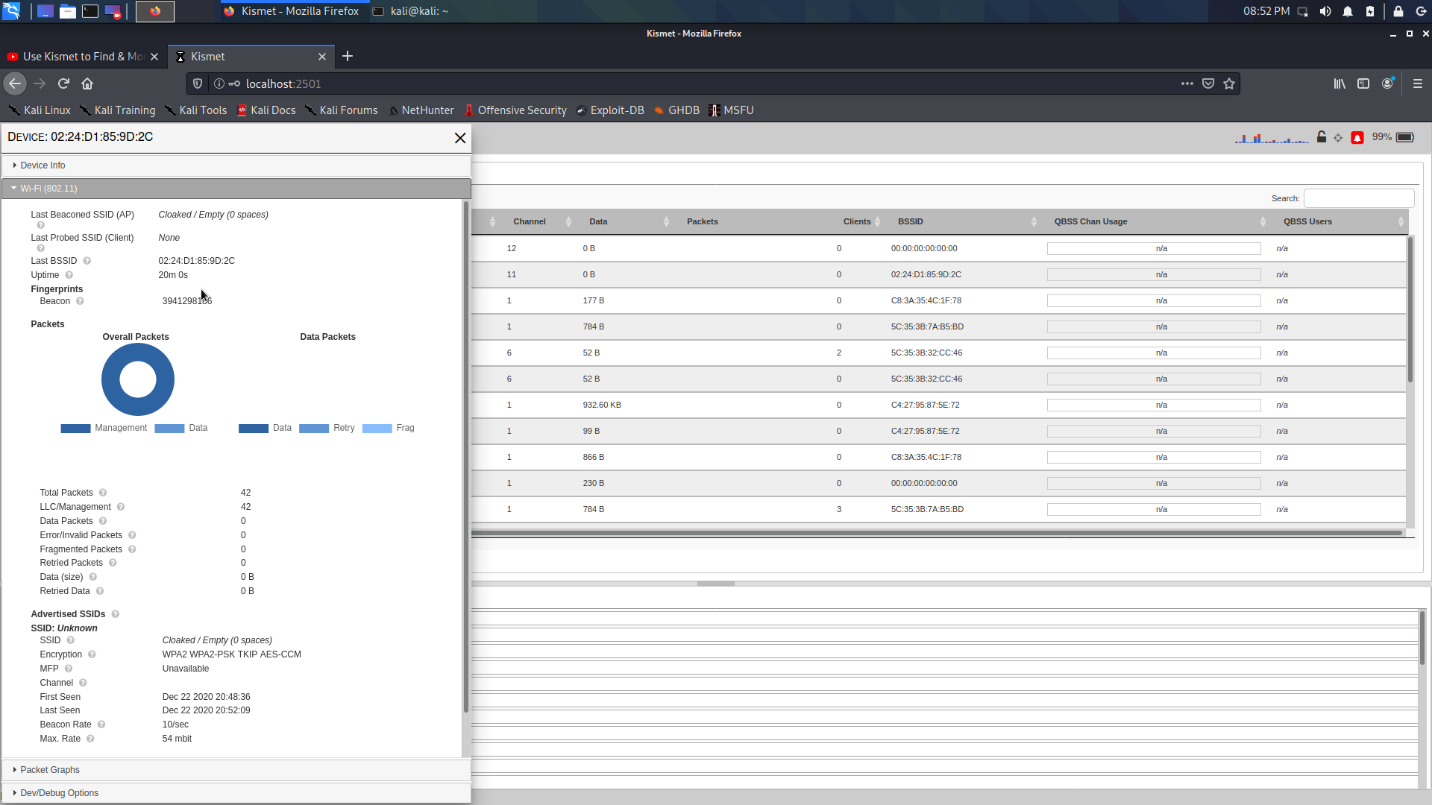


Këto mund të shihen edhe përmes terminalit po në rastin tonë I kemi shfaqur në browser.

Kismet na lejon qe te shohim edhe informacionet për një pajisje të veqantë.

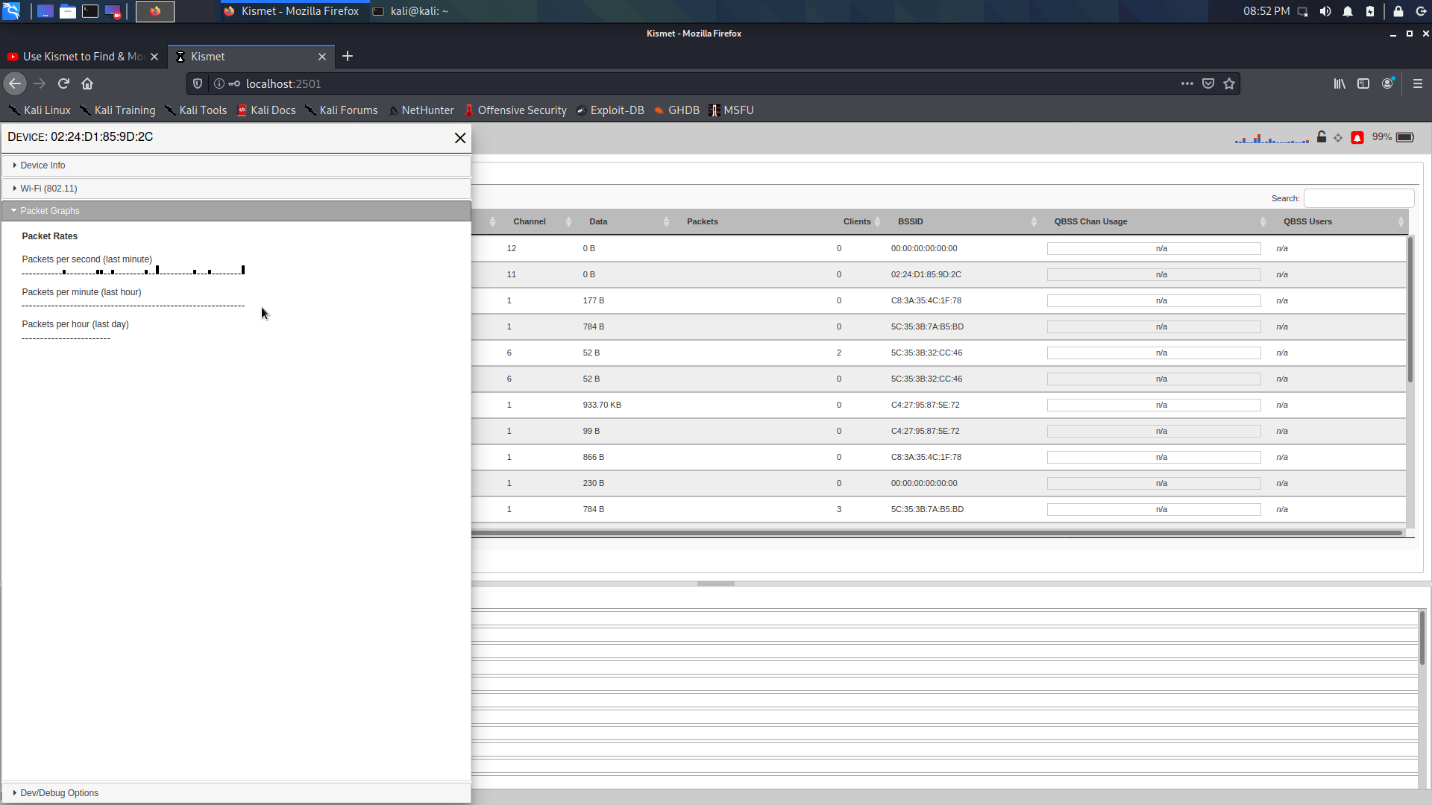


Po ashtu Kismet na lejon që të shohim edhe informacionet për një network të veqantë.



Administratorët e rrjetit dhe të sigurisë mund ta përdorin këtë veçori për të identifikuar nyjet e njohura dhe të panjohura të lidhura në rrjetin e tyre për qëllime auditimi dhe sigurie. Sulmuesit mund të synojnë këta klientë në sulmet e çertifikimit në një përpjekje për të thyer fjalëkalimet .

Kismet lejon edhe shikimin e grafeve për paketa për minuta, orë apo edhe ditë, sic është treguar në fotografi ne bazë të një shembulli.



# Përfundim

Kismet është një mjet i domosdoshëm për ta kuptuar dhe për ta pasur. Mund të mundësojë teknika të tilla si mbrojtja, hartëzimi GPS, raportimi dhe sinjalizimi i rrjetit, dhe veprime më të përparuara si injektimi i paketave dhe DOS.

Duke kuptuar Kismet dhe pikat e tij të forta, çdo profesionist i sigurisë kibernetike mund të shkojë shumë drejt kuptimit të synimit të tyre, dobësive të tij dhe asaj që një sulmues i mundshëm mund të shohë nëse ata kanë qëllime më të rrezikshme.