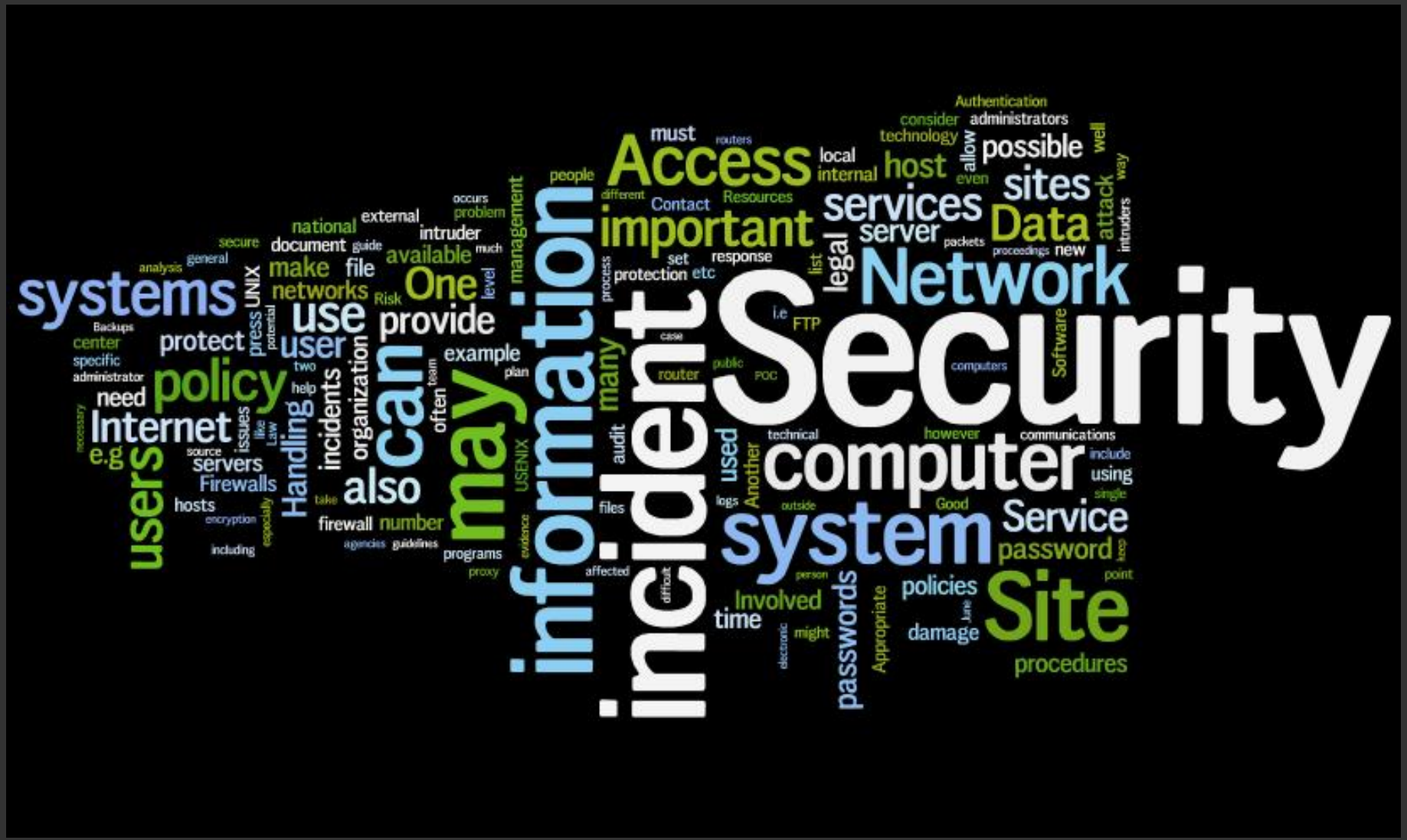
>>> Software for security tests

Name: Sofía Almeida Bruno
Fernando de la Hoz Moreno

>>> Introduction



>>> Kali Linux

* Pentesting and security auditing
* Safe development environment
* More than 300 tools

>>> Kali Linux


Applications
Places
Tue 05:10
1
Favourites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Firefox ESR
Terminal
Files
metasploit ...
armitage
burpsuite
beef xss fr...
faraday IDE
Leafpad
Tweak Tool

>>> John the Ripper

>>> John the Ripper

How does it work?

* Dictionary attack

>>> John the Ripper

How does it work?

* Password file
* Wordlist
* Compare encriptations

>>> John the Ripper

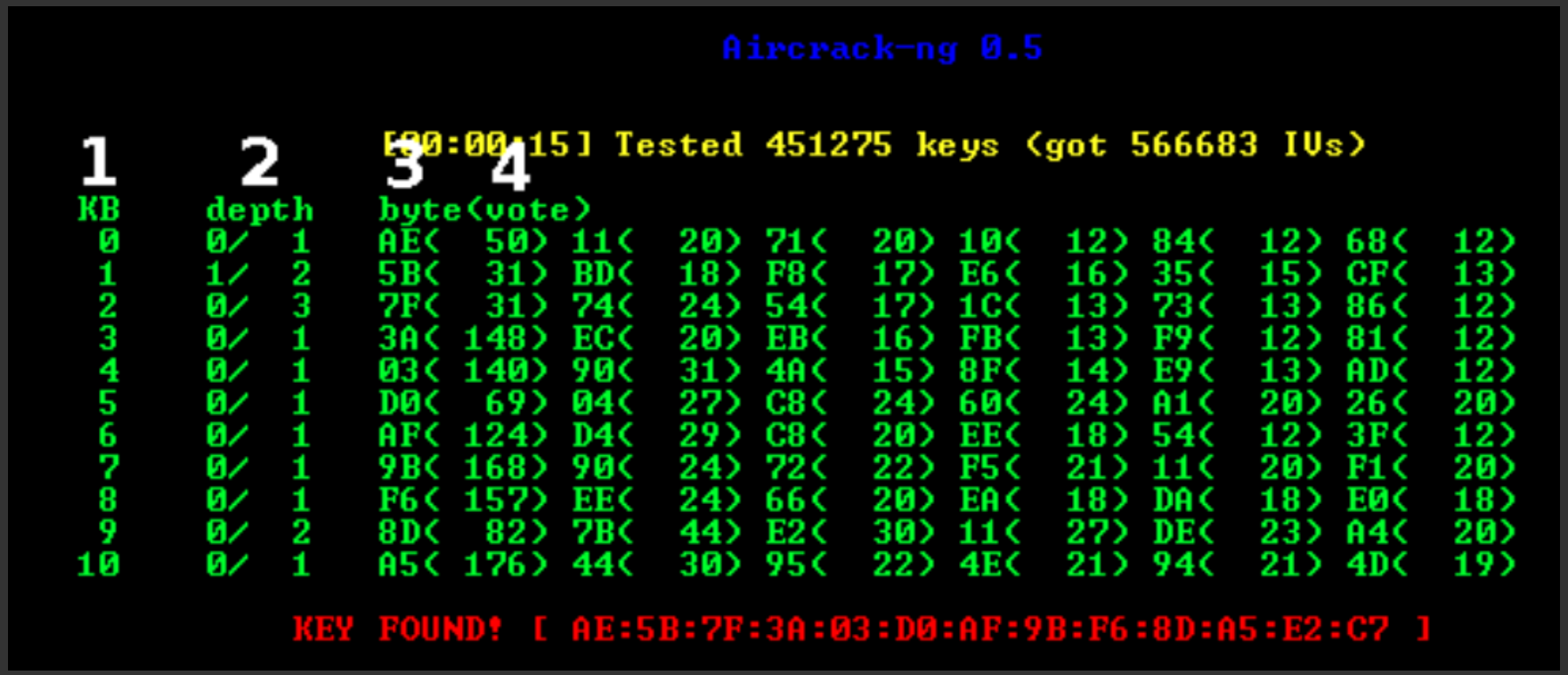
How does it work?

* Dictionary attack
* Brute force attack

>>> Aircrack-ng

>>> Aircrack-ng

Nets 802.11 WEP and WPA/WPA2-PSK

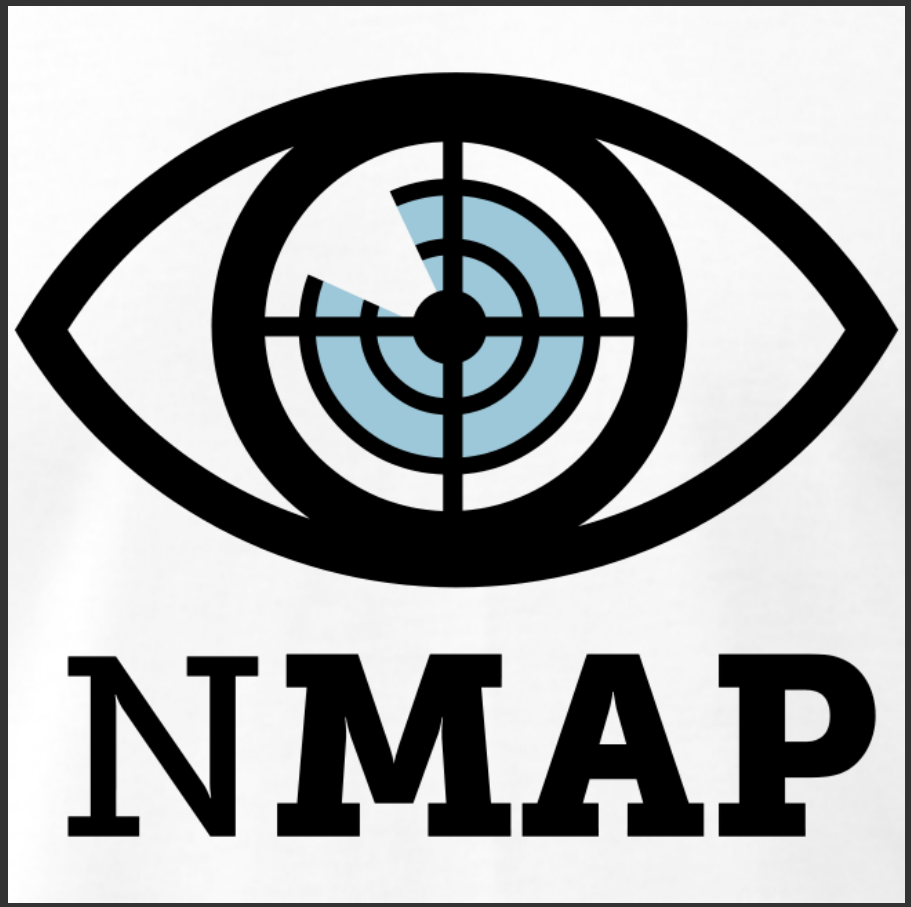


>>> Wireshark

* Network protocol analyzer
* Dynamic analysis of malware
* Intruder detection

>>> Nmap

* Host discovery
* Port analysis
* Other functionalities



>>> Nmap

Host discovery

* IP from active hosts
* Send packets

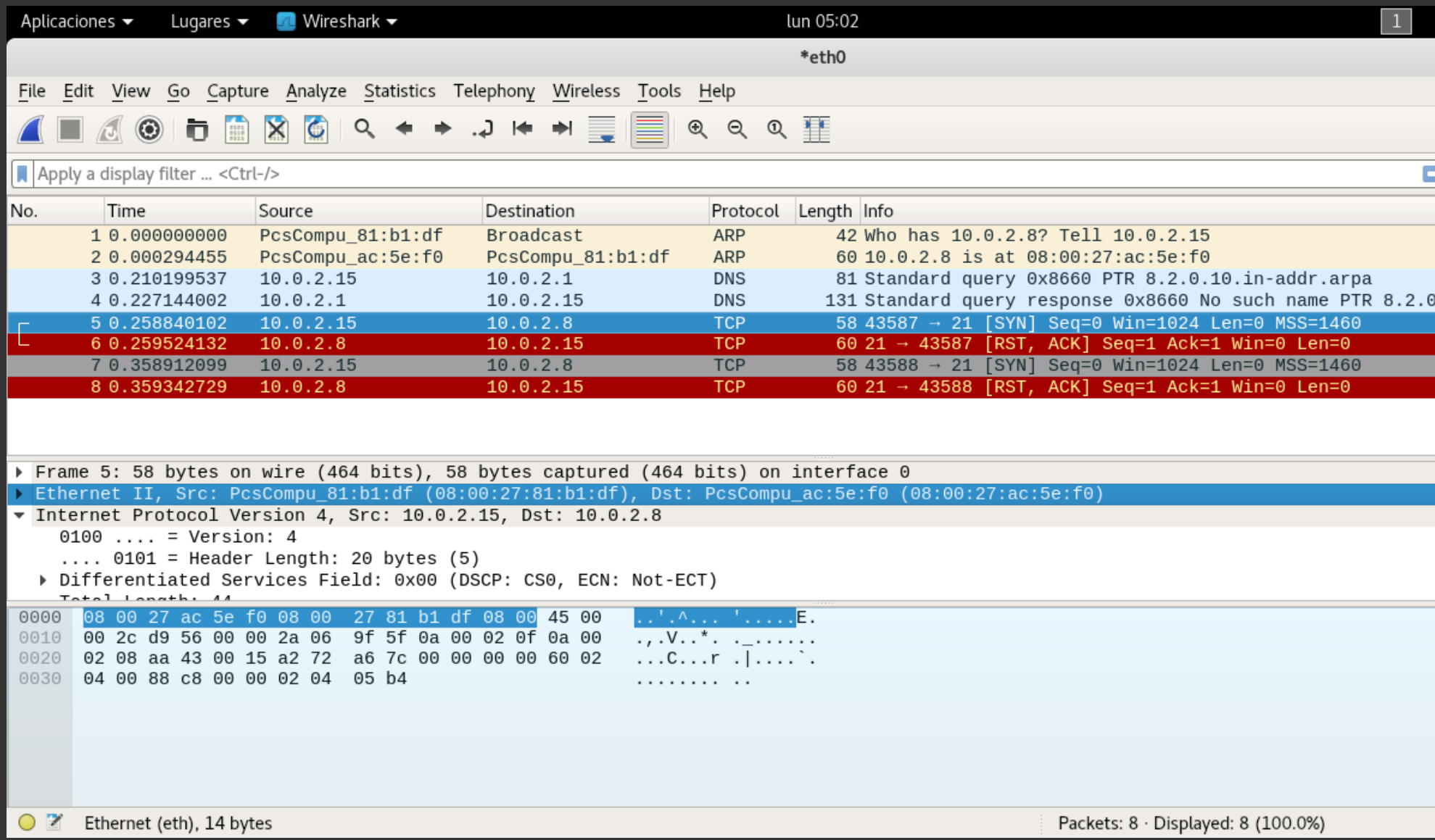
```
root@kali:~# nmap -PS -p 21 10.0.2.8
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 05:00 EST
Nmap scan report for 10.0.2.8
Host is up (0.00038s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

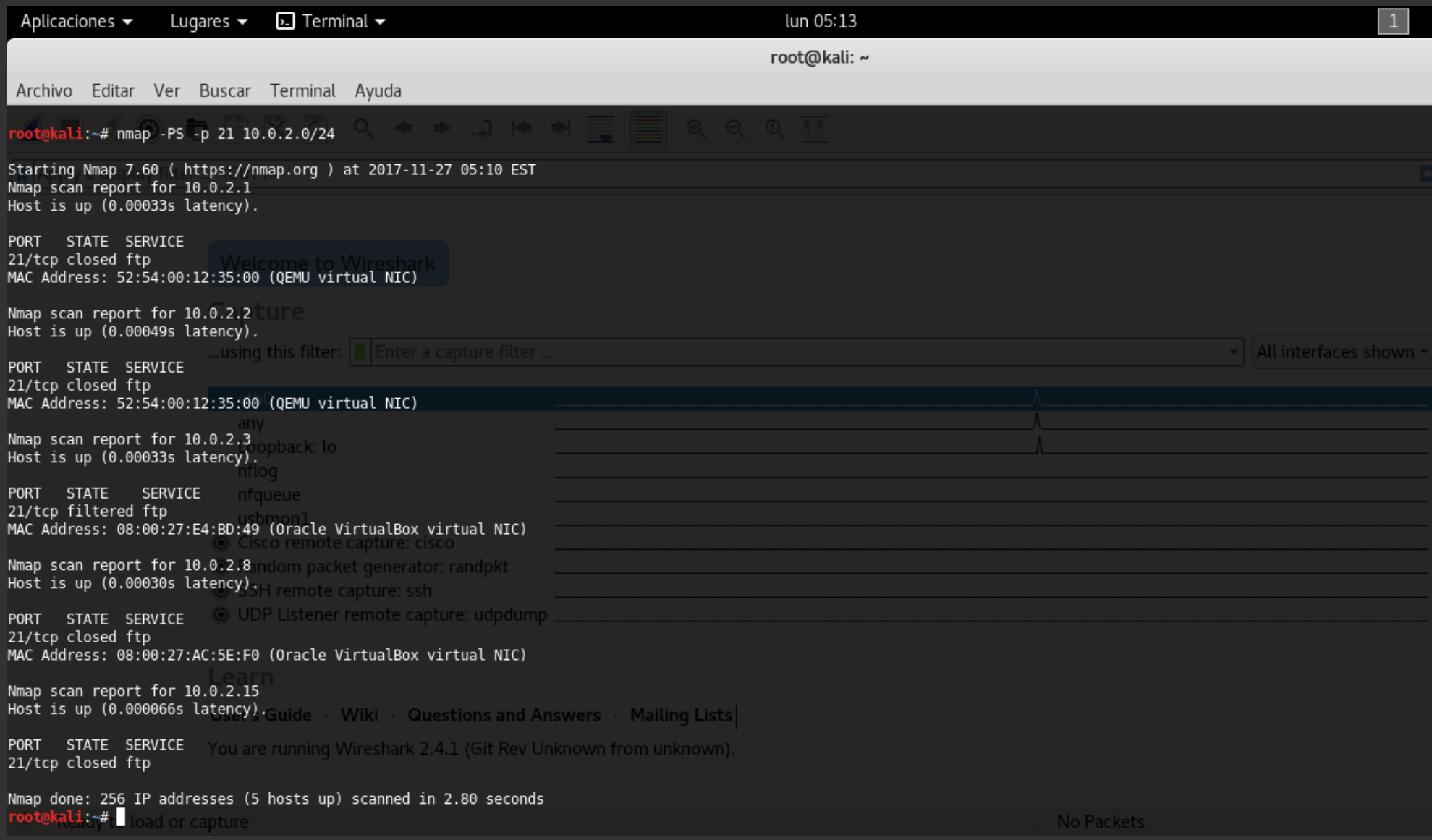
>>> Nmap

Host discovery



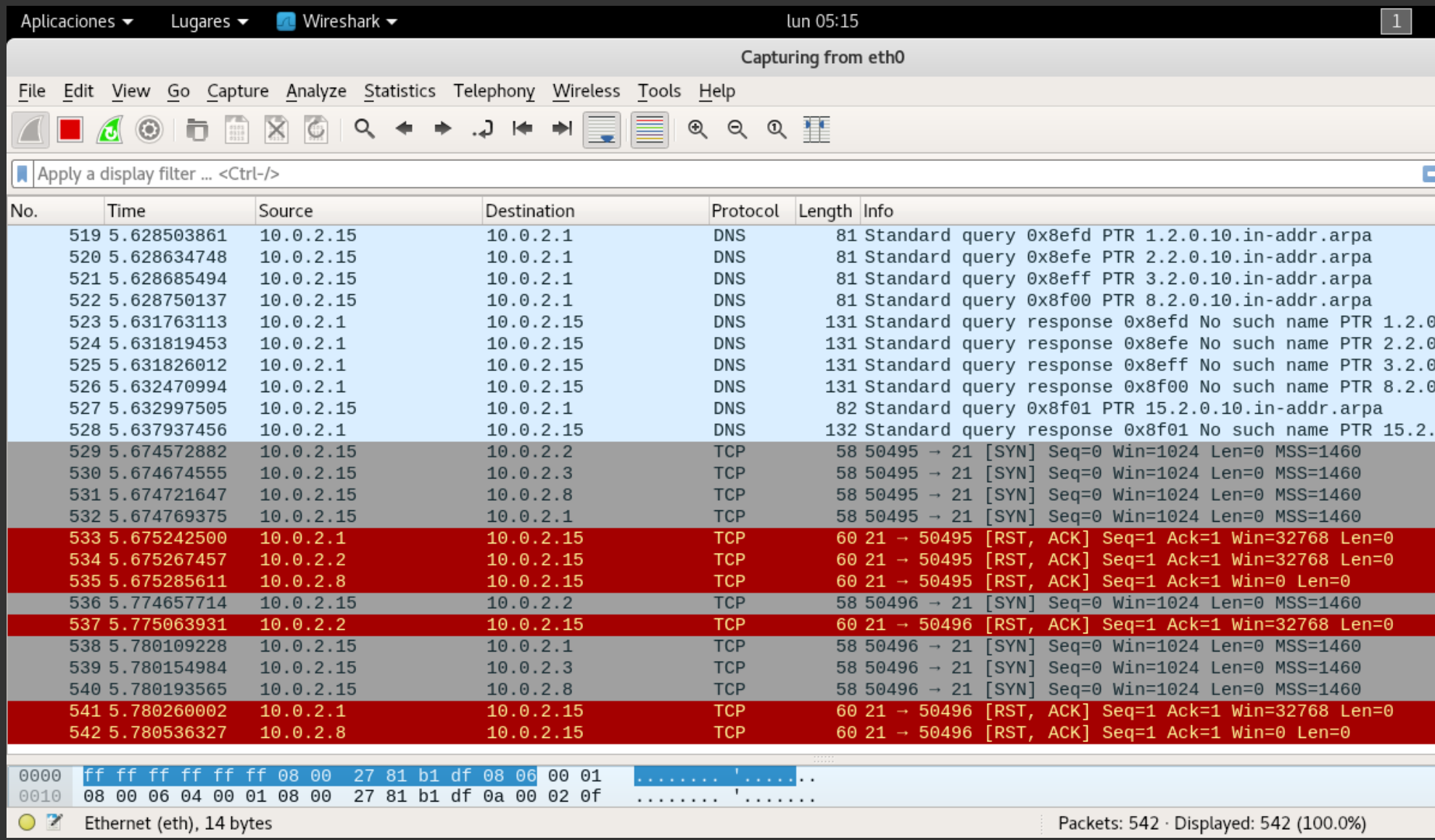
>>> Nmap

Host discovery



>>> Nmap

Host discovery



>>> Nmap

Port analysis

* Attack vector
* Send different types of packets
* Analyse the answer

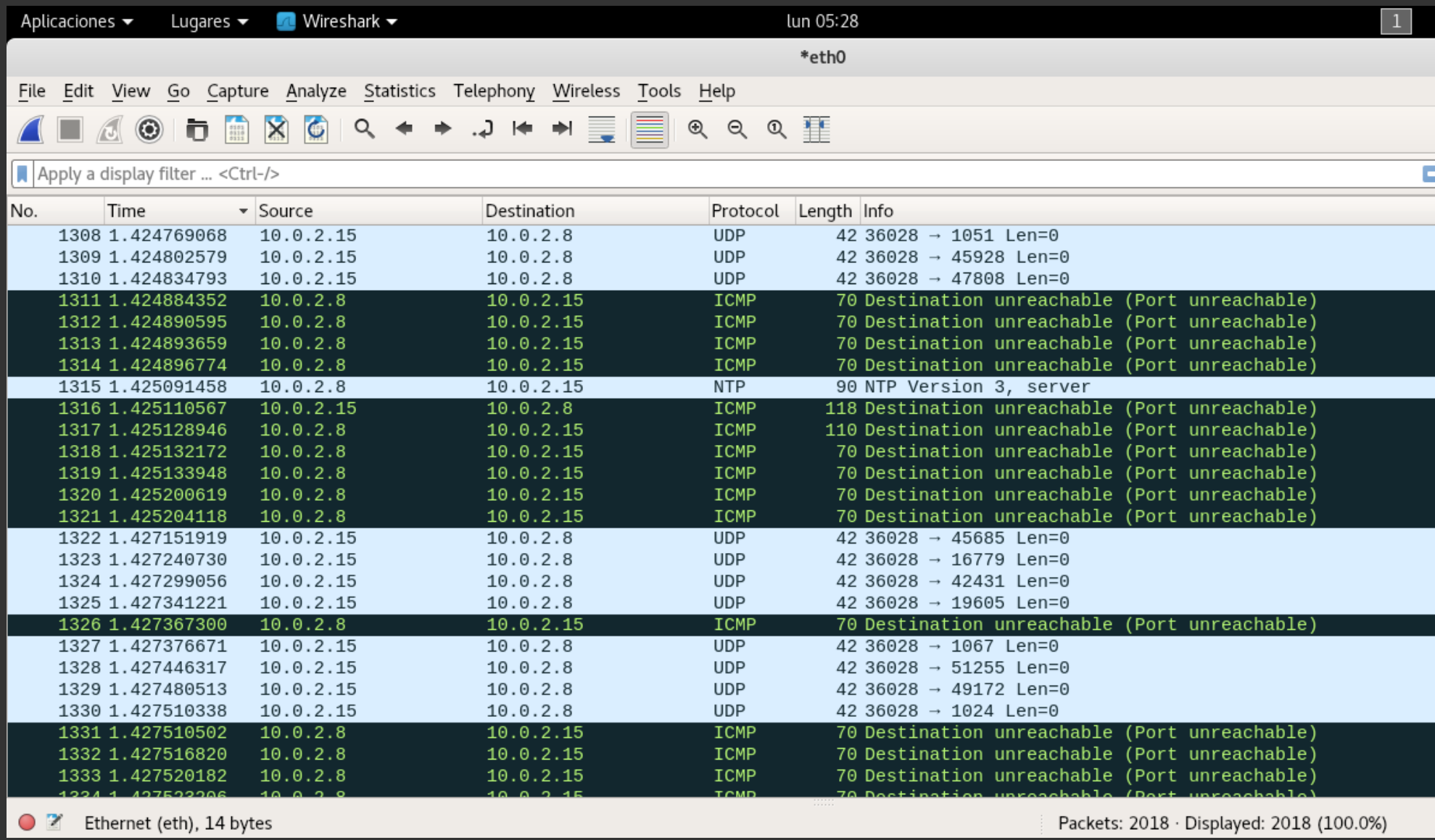
```
root@kali:~# nmap -sU  10.0.2.8

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 05:19 EST
Nmap scan report for 10.0.2.8
Host is up (0.00037s latency).
Not shown: 992 closed ports
PORT     STATE         SERVICE
123/udp  open          ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1025/udp open|filtered blackjack
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.49 seconds
```

>>> Nmap

Port analysis



>>> Metasploit

* Vulnerabilities
* Exploits
* Payloads

>>> Pros and cons

Pros:

* Security evaluation of system
* Unplanned functionalities
* Administration

Cons:

* Evil intentions
* Never completly safe

>>> Bibliography

* http://www.openwall.com/john/doc/
* https://en.wikipedia.org/wiki/John_the_Ripper
* https://nmap.org/man/es
* https://www.aircrack-ng.org/doku.php?id=aircrack-ng
* https://en.wikipedia.org/wiki/Metasploit_Project