dhcpcanon

DHCP client disclosing less identifying information.

https://github.com/dhcpap

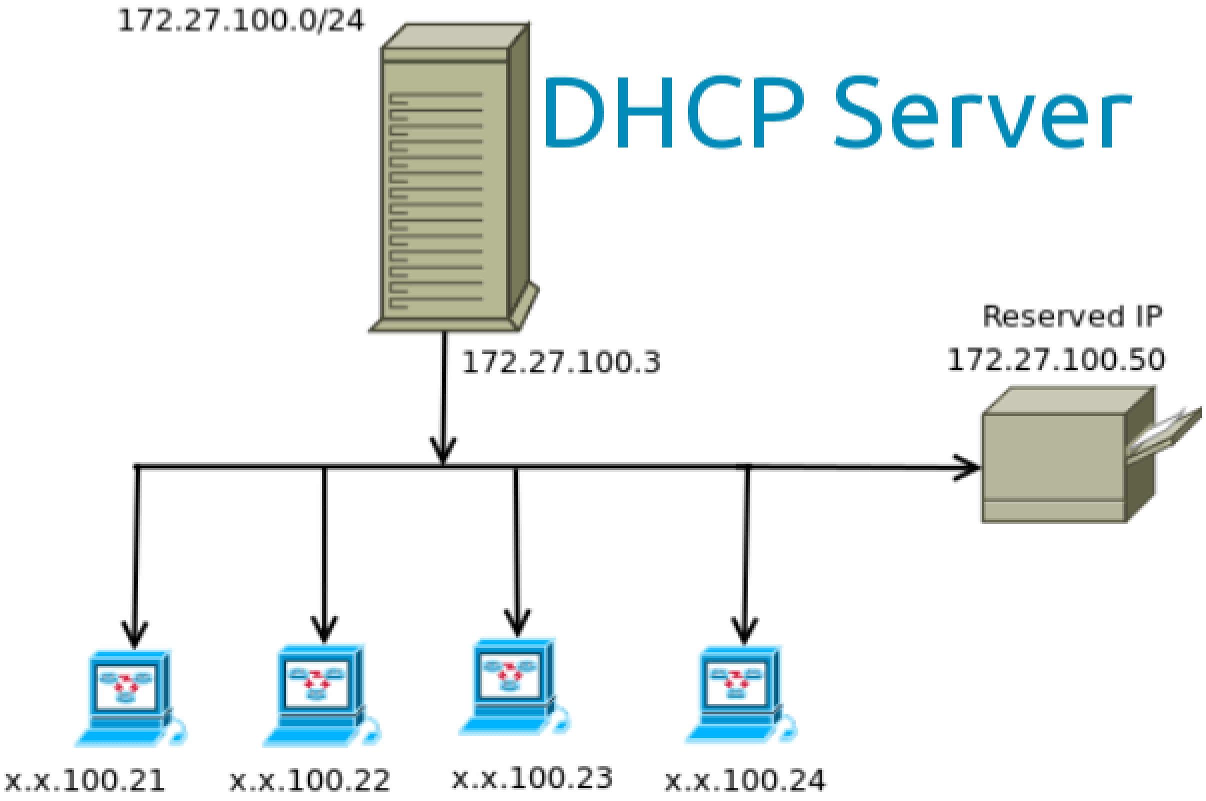
PrototypeFund demo day, Berlin, 31st August 2017

What is DHCP

Dynamic Host Configuration Protocol (DHCP)

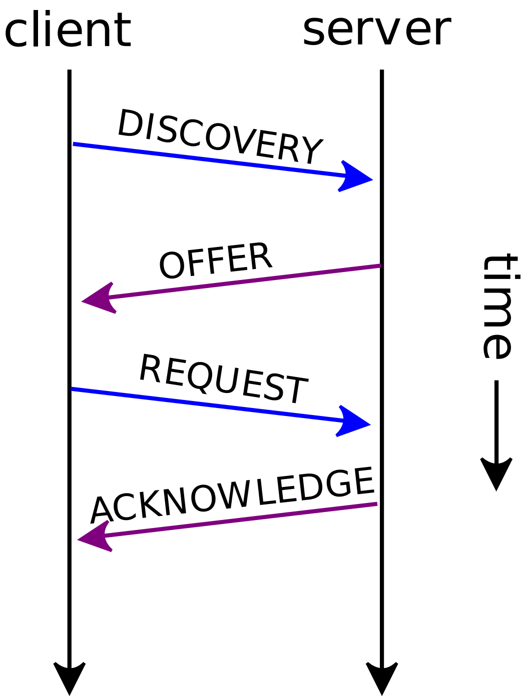
- network protocol to get IP addresses and networking parameters automatically
- transparent to the end user
- user interact with a network manager

Local network image



DHCP Server

DHCP session



1. my laptop: can i have an address?
2. server: i can offer you 192.168.1.23
3. my laptop: i request 192.168.1.23
4. server: assigned to you!

DHCP session, detailed

1. my laptop: can i have an address?
    - btw my laptop name is juga_laptop
    - it's a Dell i bought in Copenhague in 2013
    - i use Debian with dhclient version 4.3.5
    - i like the coffee with milk
2. server: i can offer you 192.168.1.23
    - btw, you can find milk in the fridge

Issues with DHCP

- reveal identifying information
- new standard to minimize it (RFC 7844)
- only a Windows 10 implementation

What I had before

python™

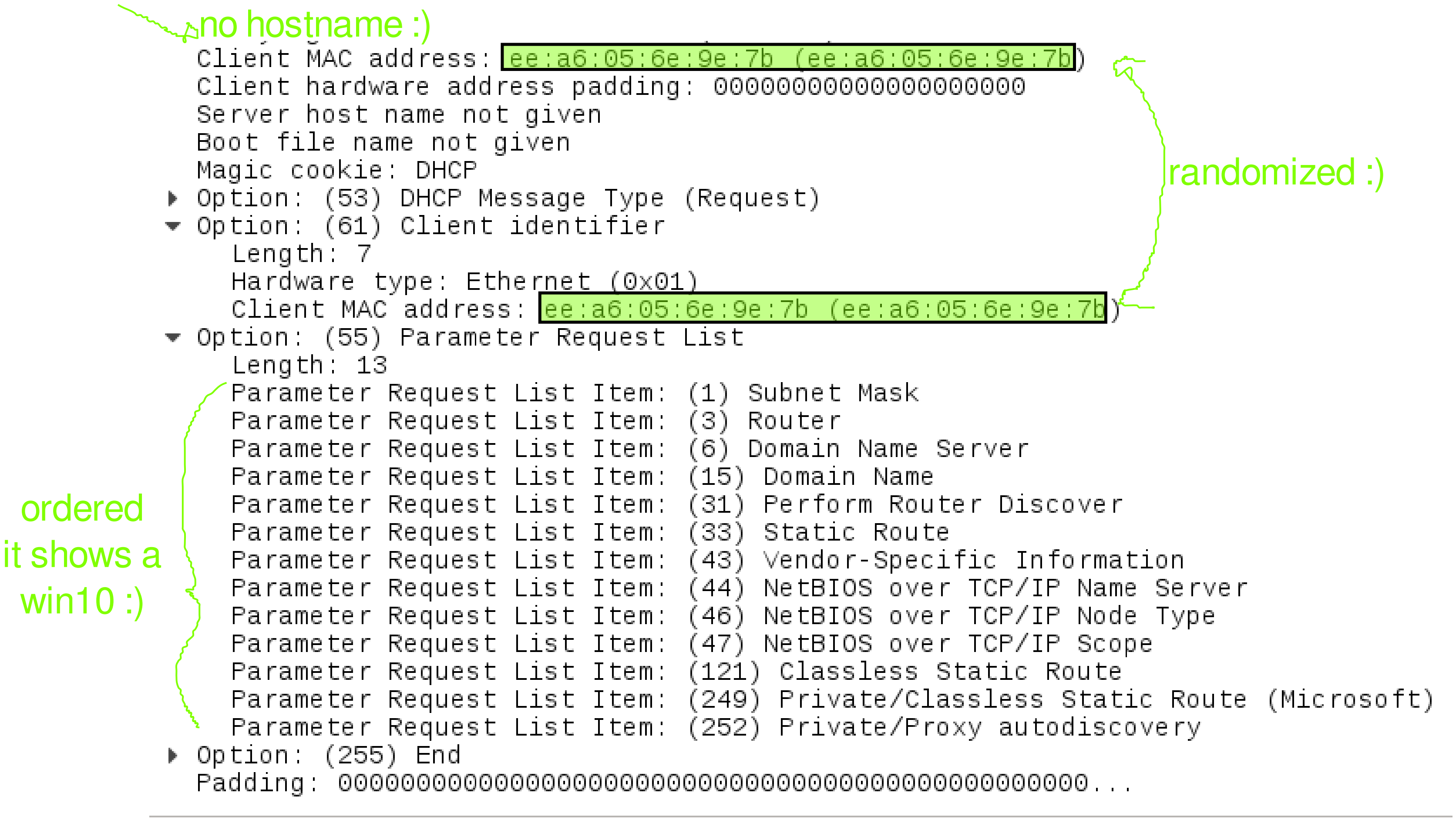
- dhcpcanon: a prototype Python DHCP client implementing part of the protocol
- ideas on how to further develop it

Achieved

dhcpcanon

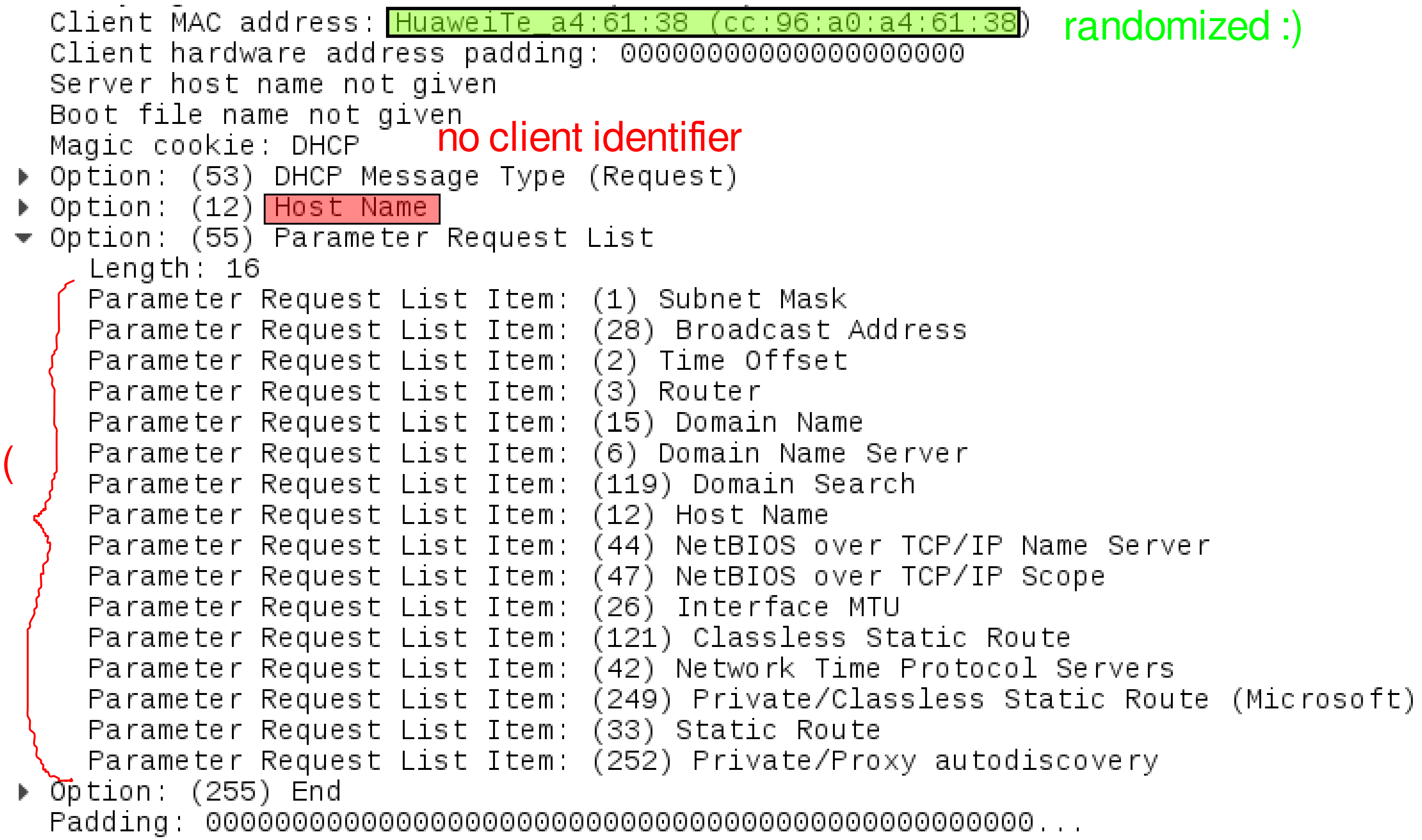
- decisions on what and how to implement: follow Windows 10 implementation instead of restricted version of RFC 7844
- complete the protocol
- automatic testing
- improve documentation
- Debian package
- contact with different Linux distributions to test it

Example Windows 10 capture



```
    Client MAC address: ee:a6:05:6e:9e:7b (ee:a6:05:6e:9e:7b)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Request)
  ▾ Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: ee:a6:05:6e:9e:7b (ee:a6:05:6e:9e:7b)
  ▾ Option: (55) Parameter Request List
      Length: 13
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (31) Perform Router Discover
      Parameter Request List Item: (33) Static Route
      Parameter Request List Item: (43) Vendor-Specific Information
      Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
      Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
      Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
      Parameter Request List Item: (121) Classless Static Route
      Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
      Parameter Request List Item: (252) Private/Proxy autodiscovery
  ▸ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000...
```

Example `dhclient` capture



```
 Client MAC address: HuaweiTe_a4:61:38 (cc:96:a0:a4:61:38)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Request)
▶ Option: (12) Host Name
▼ Option: (55) Parameter Request List
    Length: 16
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (2) Time Offset
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (252) Private/Proxy autodiscovery
▶ Option: (255) End
 Padding: 000000000000000000000000000000000000000000000000...
```

randomized :)

no client identifier

unordered :(

`systemd` (system manager)

- modified DHCP client code to enable Anonymity Profiles
- code in the process of being merge by `systemd` team

`Gnome Network Manager` (network manager)

Developing a proper integration in process

`dhcpcfp`

A network scanner to show:

- which is the identifying information can be found
- how is different to the Anonymity profiles
- how operating system, device and/or person can be guessed

Internet Engineering Task Force meeting

IETF

- suggestions from the main author of the RFC 7844

Bornhack hacker camp

Bornhack

- presentation: feedback and interesting ideas
- workshop: catch bugs

Linux distribution communities

Interest on integrating `dhcpcanon`: Debian, Tails, Subgraph, Gentoo, Archlinux

Learned

Worth to remember

- *release early, release often*
- *divide and conquer* (on tasks)
- is fun and productive to work with others
- challenging to explain technical concepts to non technical users

New

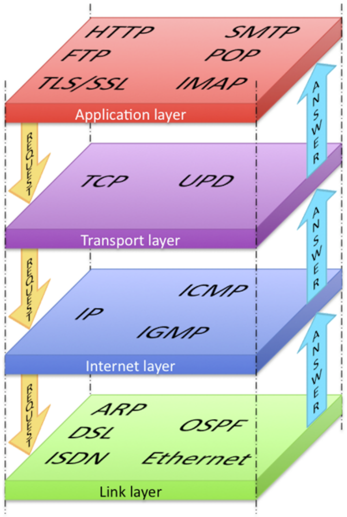
- present earlier to get feedback and bug reports earlier
- strategies to develop awareness (thanks marketing coaching!!)

IETF community

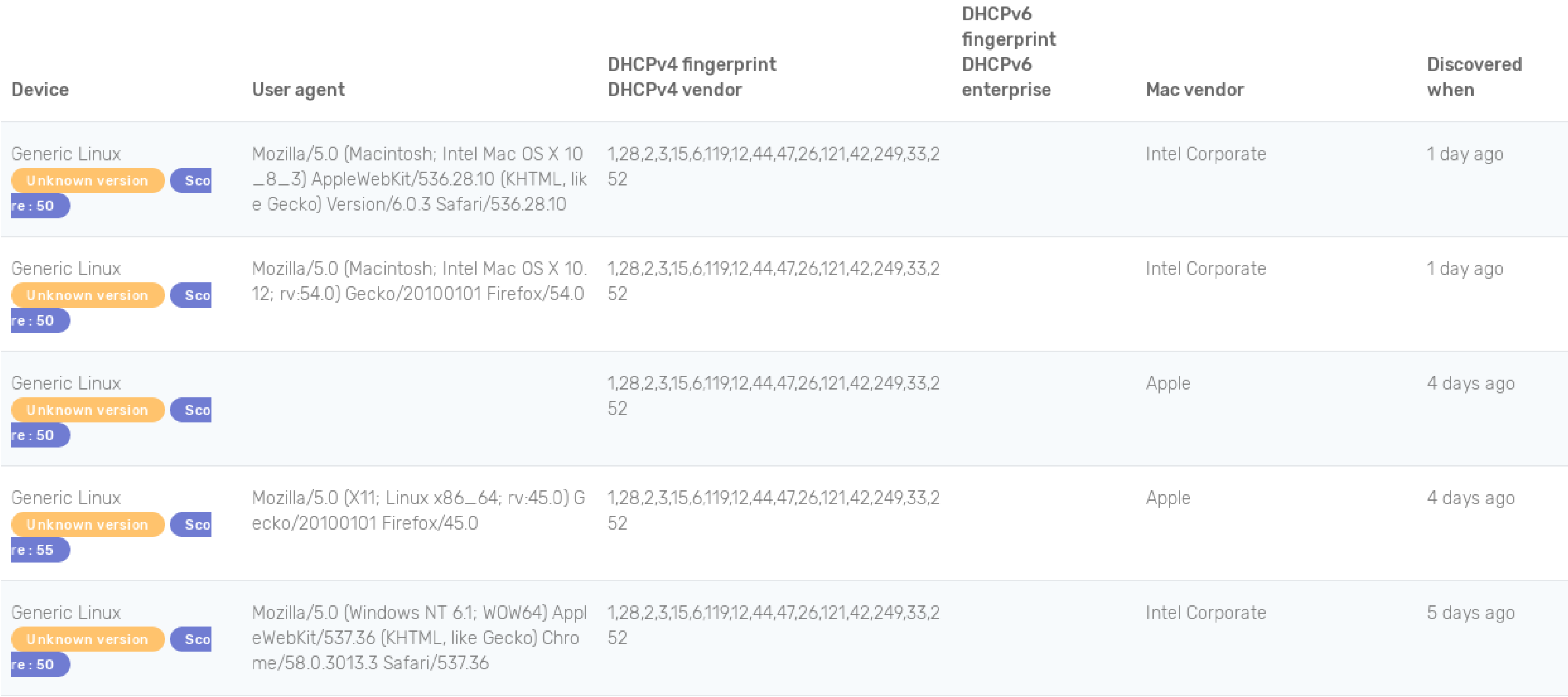
- worldwide open standards organization
- anyone can participate
- though difficult without funding nor corporate sponsor
- *rough consensus and working code*

Internet protocols development

- political and historical reasons
- how the need for the Anonymity Profiles actually happens



DHCP fingerprint databases



Device	User agent	DHCPv4 fingerprint DHCPv4 vendor	DHCPv6 fingerprint DHCPv6 enterprise	Mac vendor	Discovered when
Generic Linux Unknown version Score : 50	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/536.28.10 (KHTML, like Gecko) Version/6.0.3 Safari/536.28.10	1,28,2,3,15,6,119,12,44,47,26,121,42,249,33,252		Intel Corporate	1 day ago
Generic Linux Unknown version Score : 50	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0	1,28,2,3,15,6,119,12,44,47,26,121,42,249,33,252		Intel Corporate	1 day ago
Generic Linux Unknown version Score : 50		1,28,2,3,15,6,119,12,44,47,26,121,42,249,33,252		Apple	4 days ago
Generic Linux Unknown version Score : 55	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0	1,28,2,3,15,6,119,12,44,47,26,121,42,249,33,252		Apple	4 days ago
Generic Linux Unknown version Score : 50	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3013.3 Safari/537.36	1,28,2,3,15,6,119,12,44,47,26,121,42,249,33,252		Intel Corporate	5 days ago

Did not work as planned

- planning :(
- the protocol and integration with operating systems can be more complex than i knew or expected

What is next

dhcpcanon, systemd

- more people to test it to be ready for end users
- further development (IPv6)
- further operating systems compatibility (WIP)
- further documentation

Others

- domain and Web page to facilitate finding documentation (WIP)
- final report
- more presentations and/or worshops
- Raspberry Pi image for demonstration purposes

Other operating systems implementations

Android, FreeBSD, Mac OS, iOS...

Thank you very much!

Many people for their very valuable ideas and suggestions.

Excelent PrototypeFund team :-)

Federal Ministry
of Education
and Research

Contact

juga at riseup dot net

2DA8 1D01 455C 3A00 3219 8850 F305 447A F806 D46B

IRC: #dhcpcanon at havana.baconsvin.org:6697