Infoblox
CONTROL YOUR NETWORK

DHCPv6 Fingerprinting and BYOD

Tom Coffeen, IPv6 Evangelist

NANOG 59 - Chandler, Arizona

Agenda

1. What is BYOD and why is it important?
2. What is DHCP(v6) fingerprinting?
3. How does DHCP fingerprinting works in IPv4?
4. Information about DHCP fingerprinting data
5. Benefit of DHCP(v6) fingerprinting
6. Differences in how DHCPv6 fingerprinting works
7. The potential value of building an open DHCPv6 fingerprint database

So, you've been living under a rock (or working for an SP)

BYOD is:

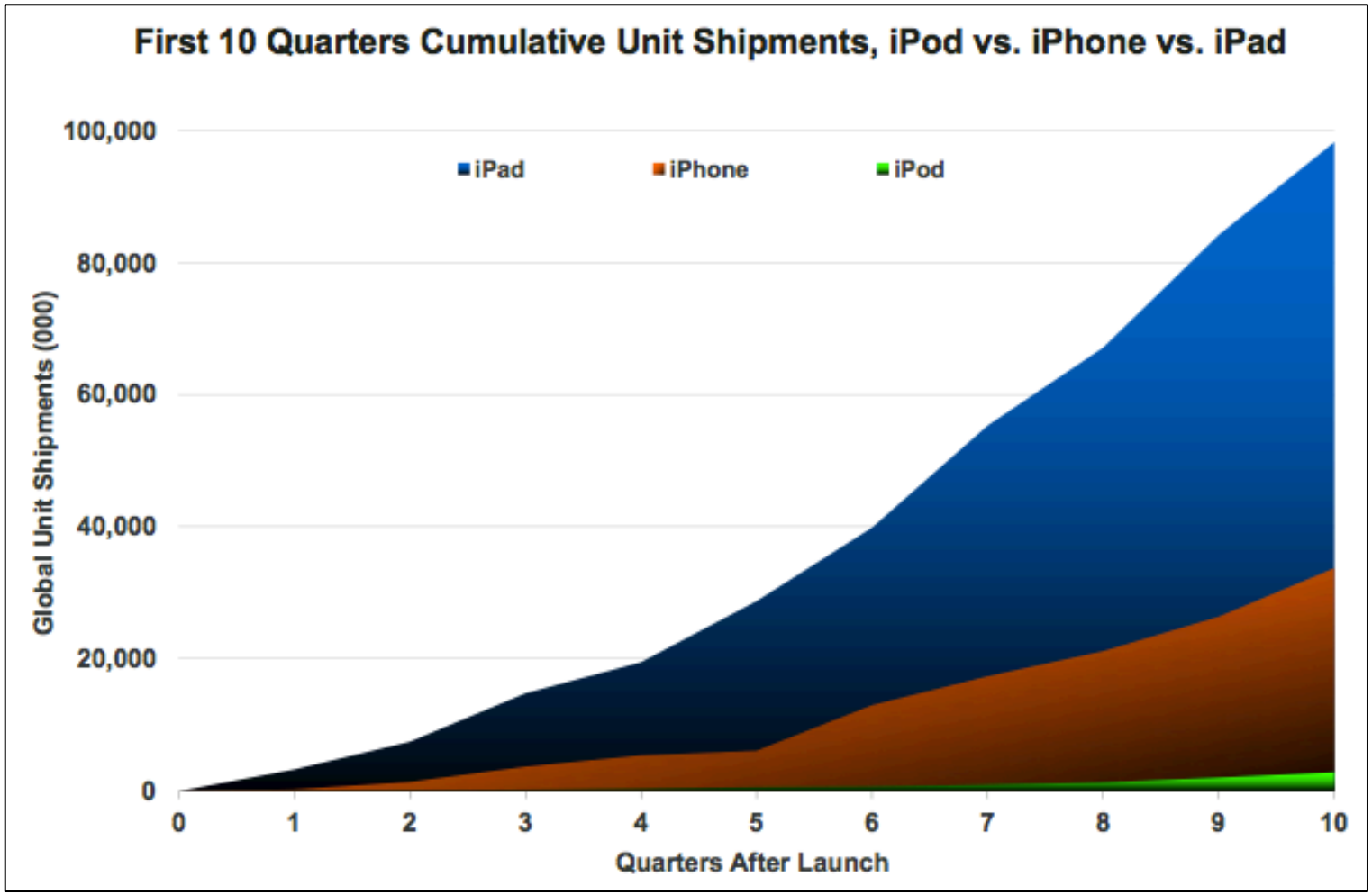
a) The latest hip hop sensation from Slovenia

b) General Zod's little brother from the planet Krypton

c) Line four on the eye chart

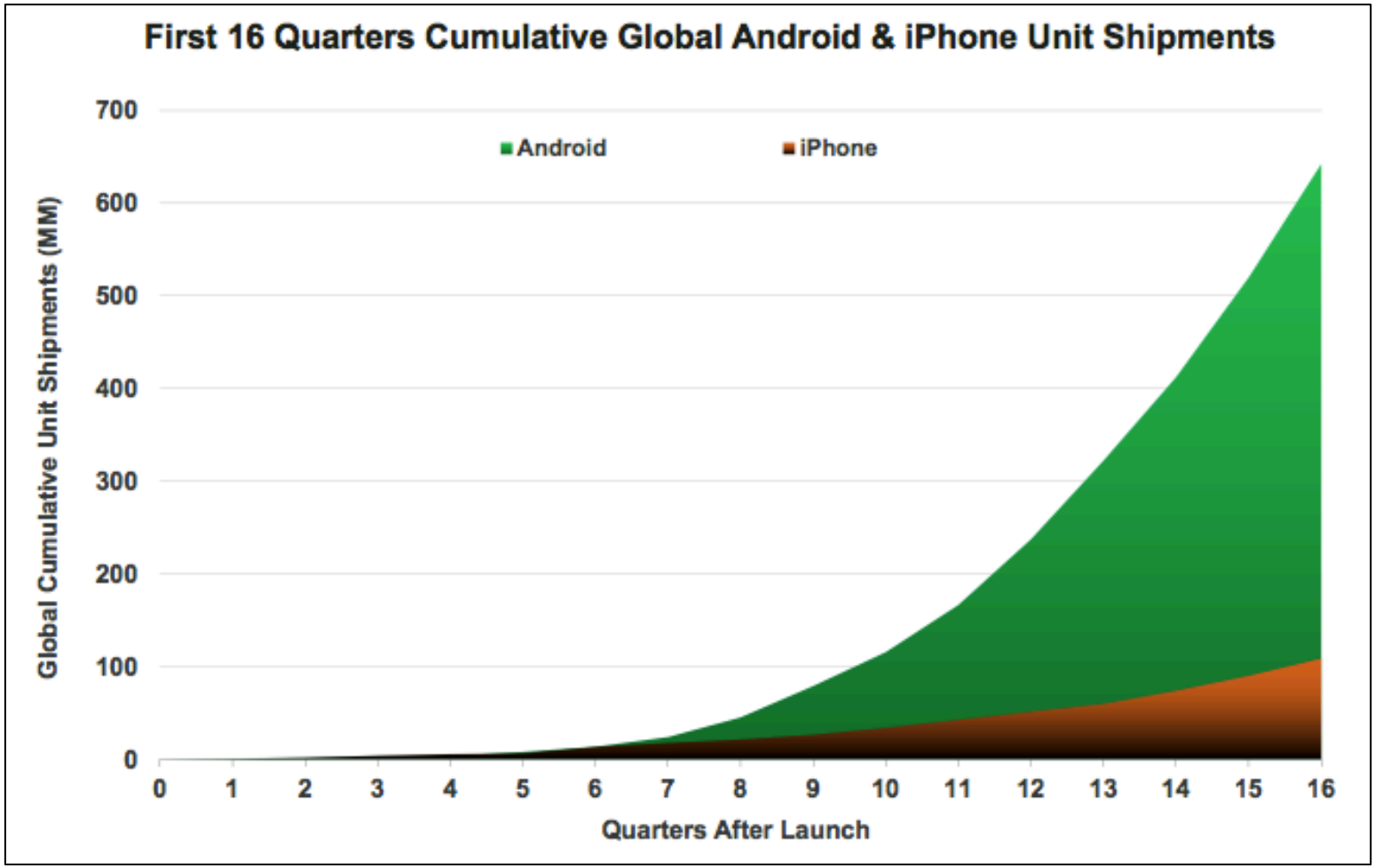
d) An abbreviation for "bring your own device"; i.e., end user personal devices on the corporate network

Why the BYOD challenge is coming to an enterprise near you



Source: Mary Meeker, Internet Trends @Stanford – Bases 12/03/2012

Why the BYOD challenge is coming to an enterprise near you



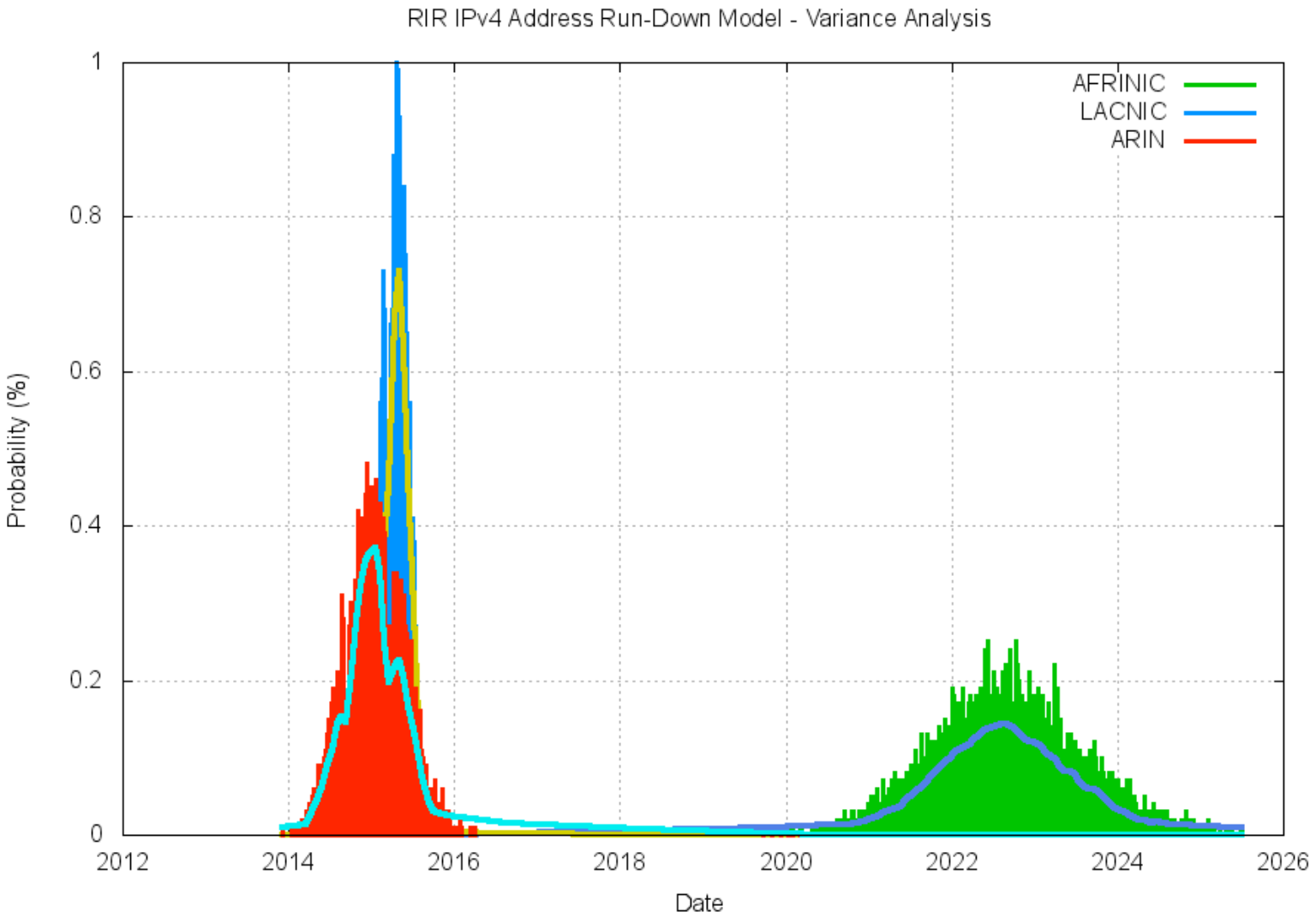
Source: Mary Meeker, Internet Trends @Stanford – Bases 12/03/2012

What does massive device proliferation look like?

This slide is awesome

$$4{,}294{,}967{,}296 < 7{,}000{,}000{,}000$$

And why the BYOD challenge will include IPv6

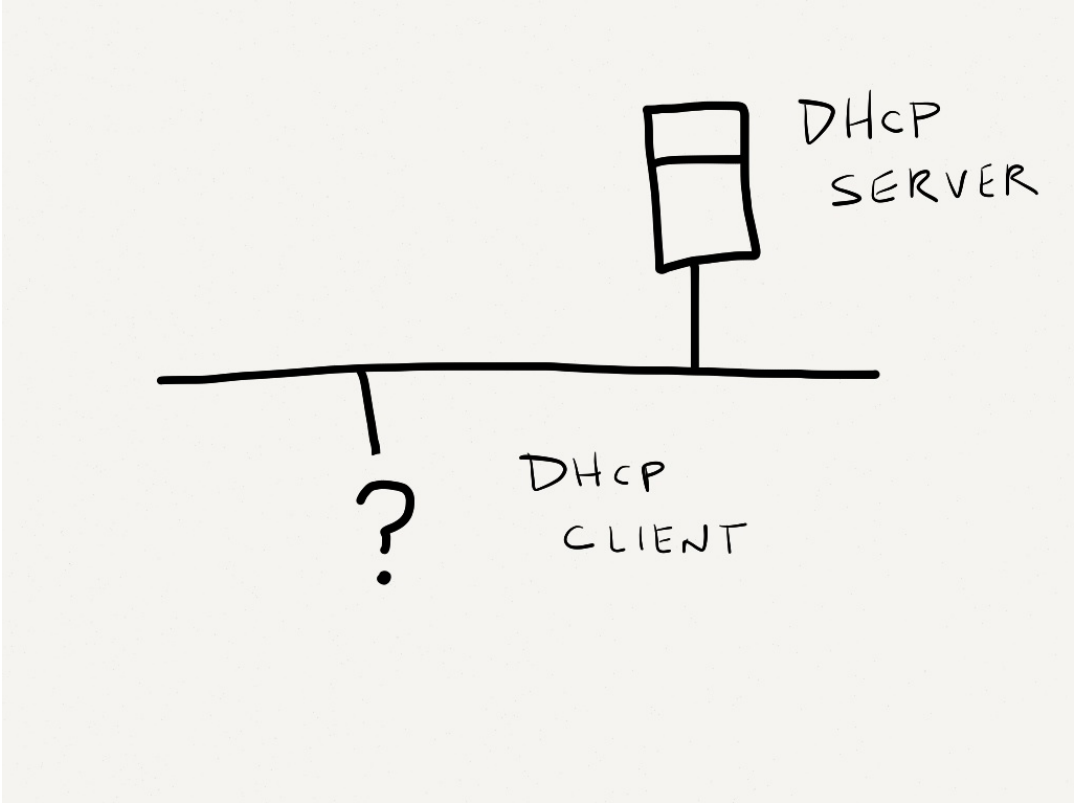


Source: Geoff Huston IPv4 Address Report, 9/24/2013

DHCP Fingerprinting

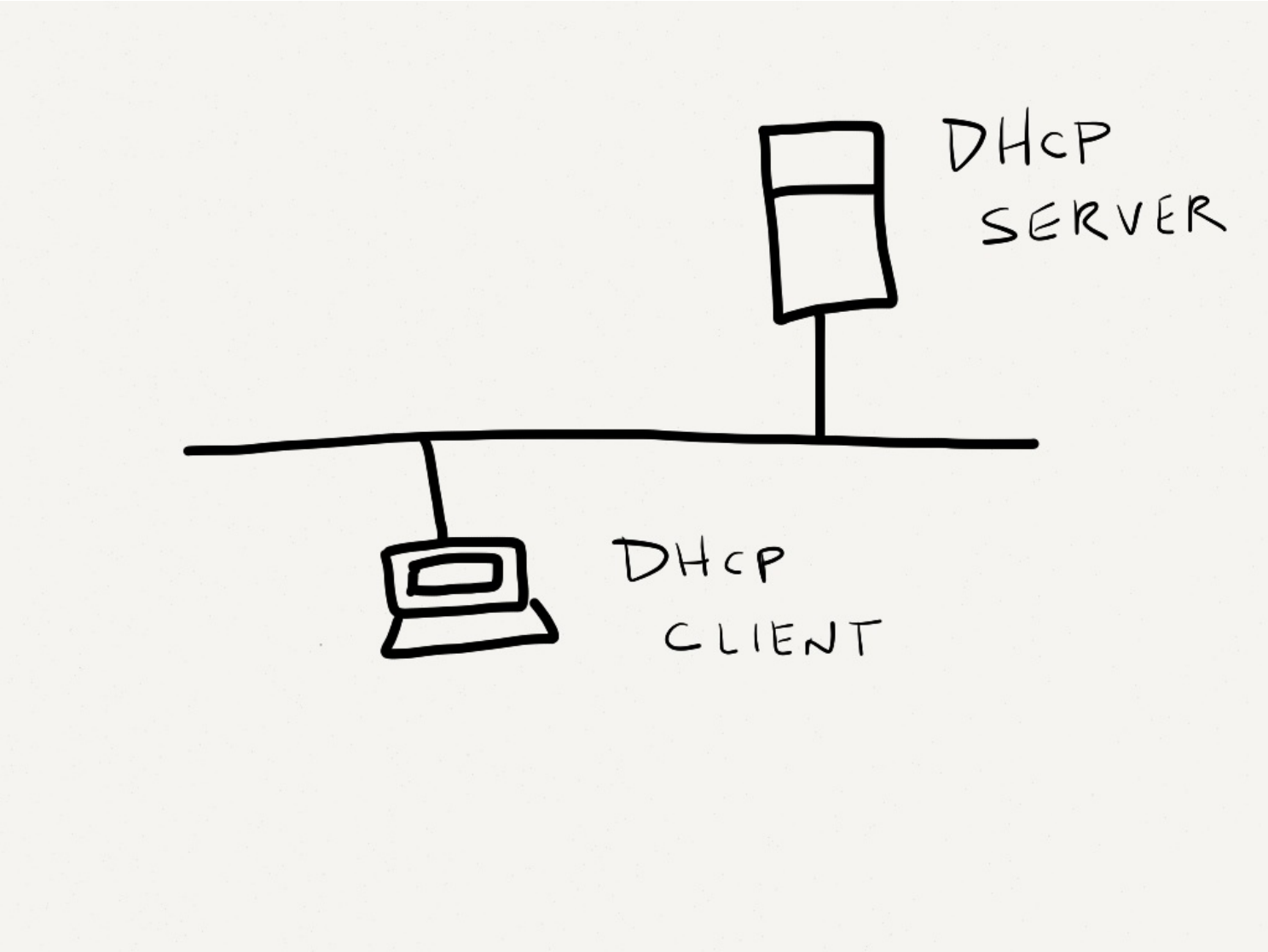
What is DHCP fingerprinting?

DHCP Fingerprinting

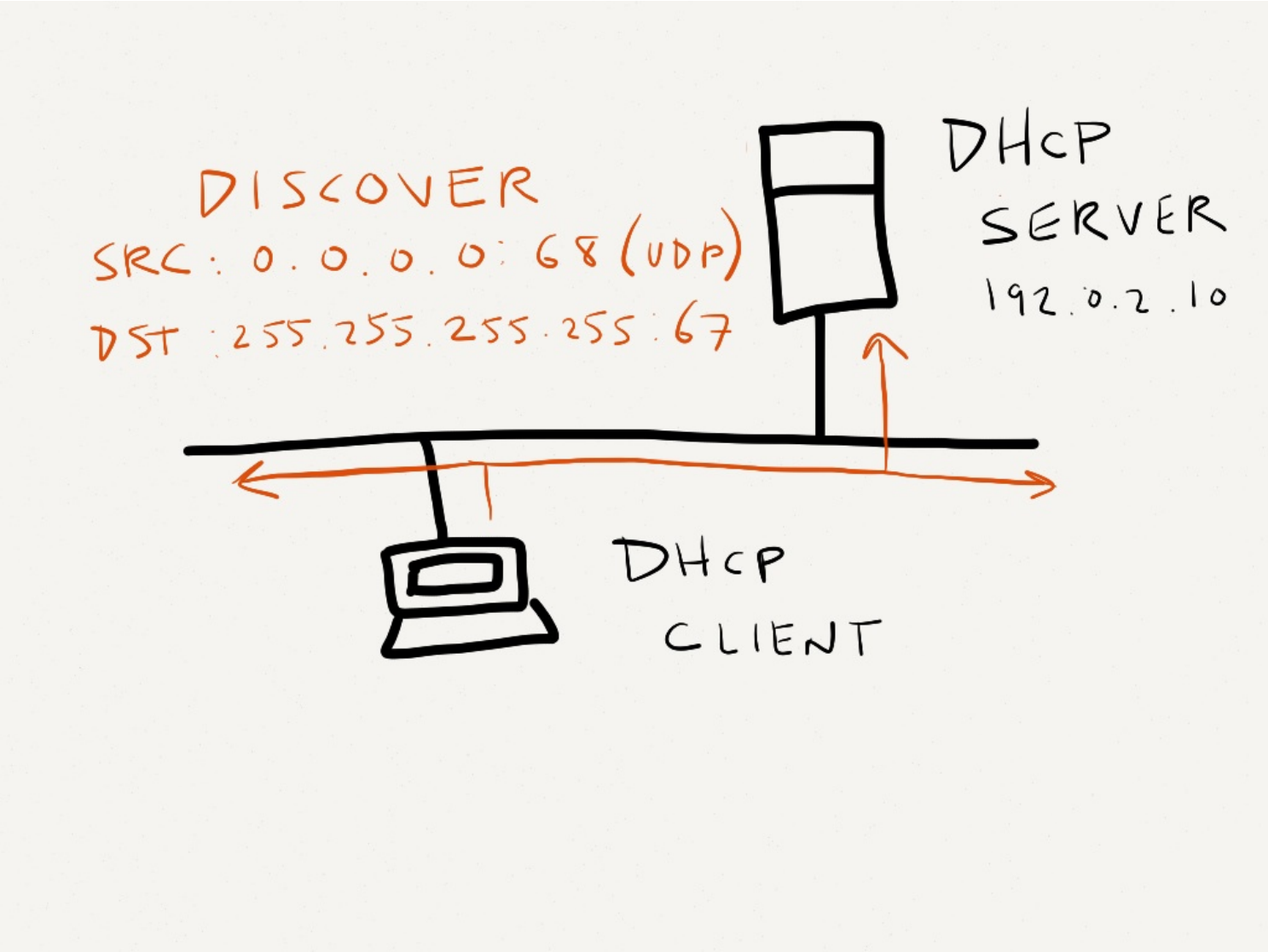


The goal is to determine the client type using only data from a basic DHCP transaction

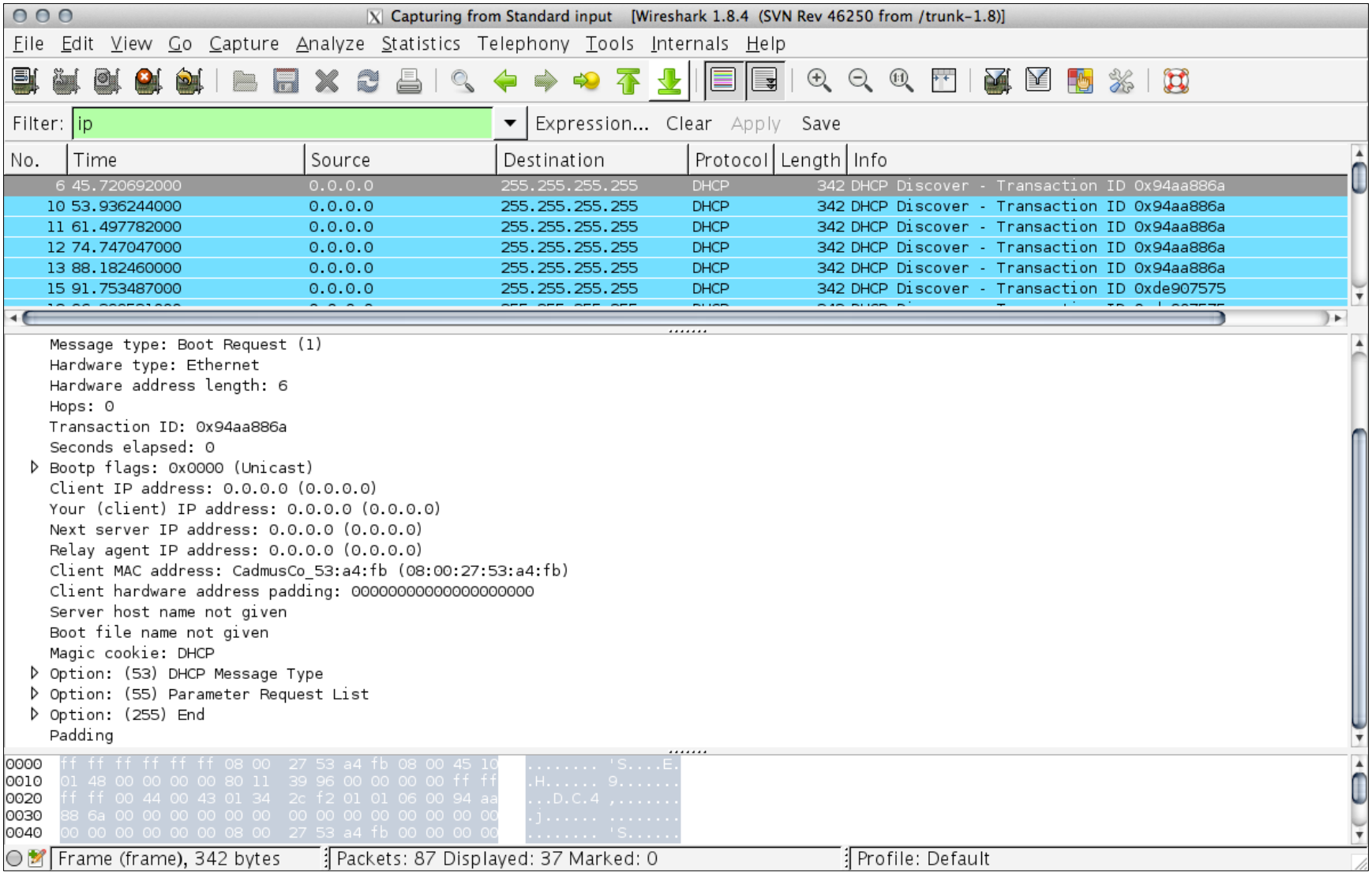
DHCP Transaction



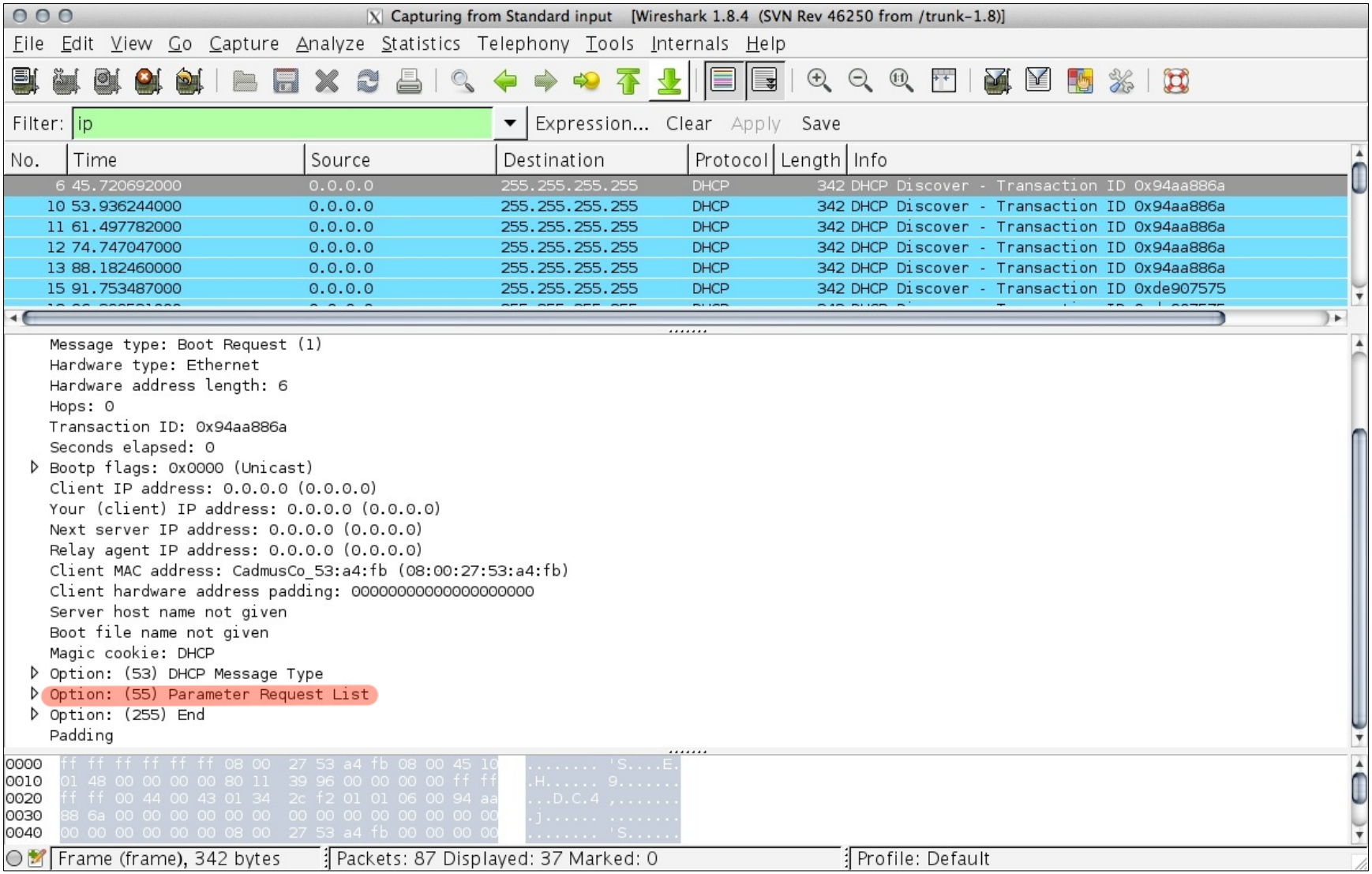
DHCP Transaction



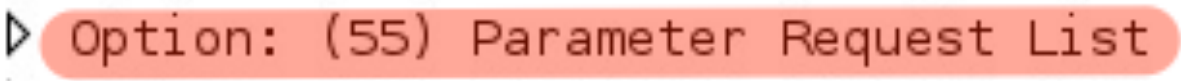
DHCP Fingerprinting



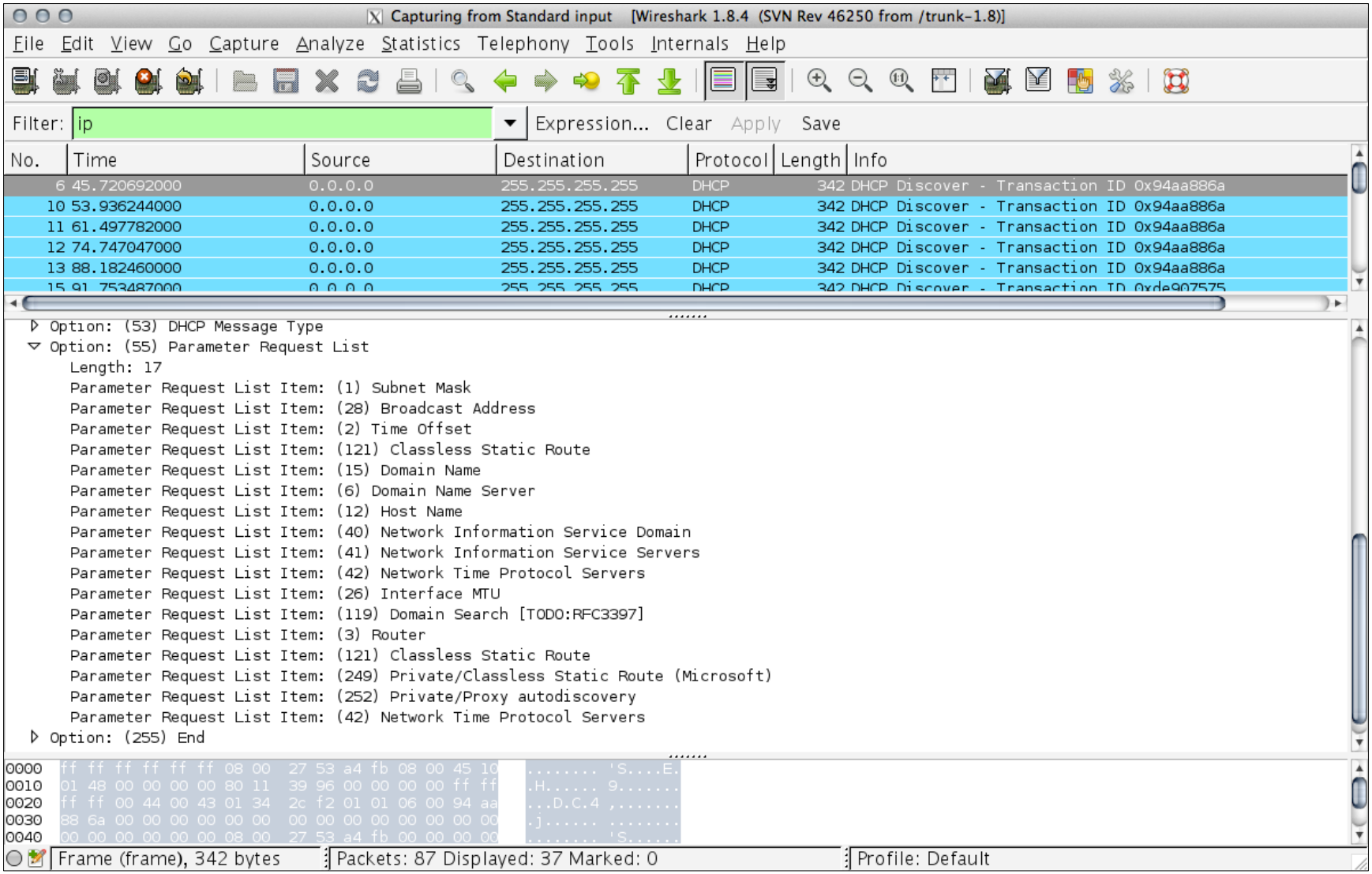
DHCP Fingerprinting



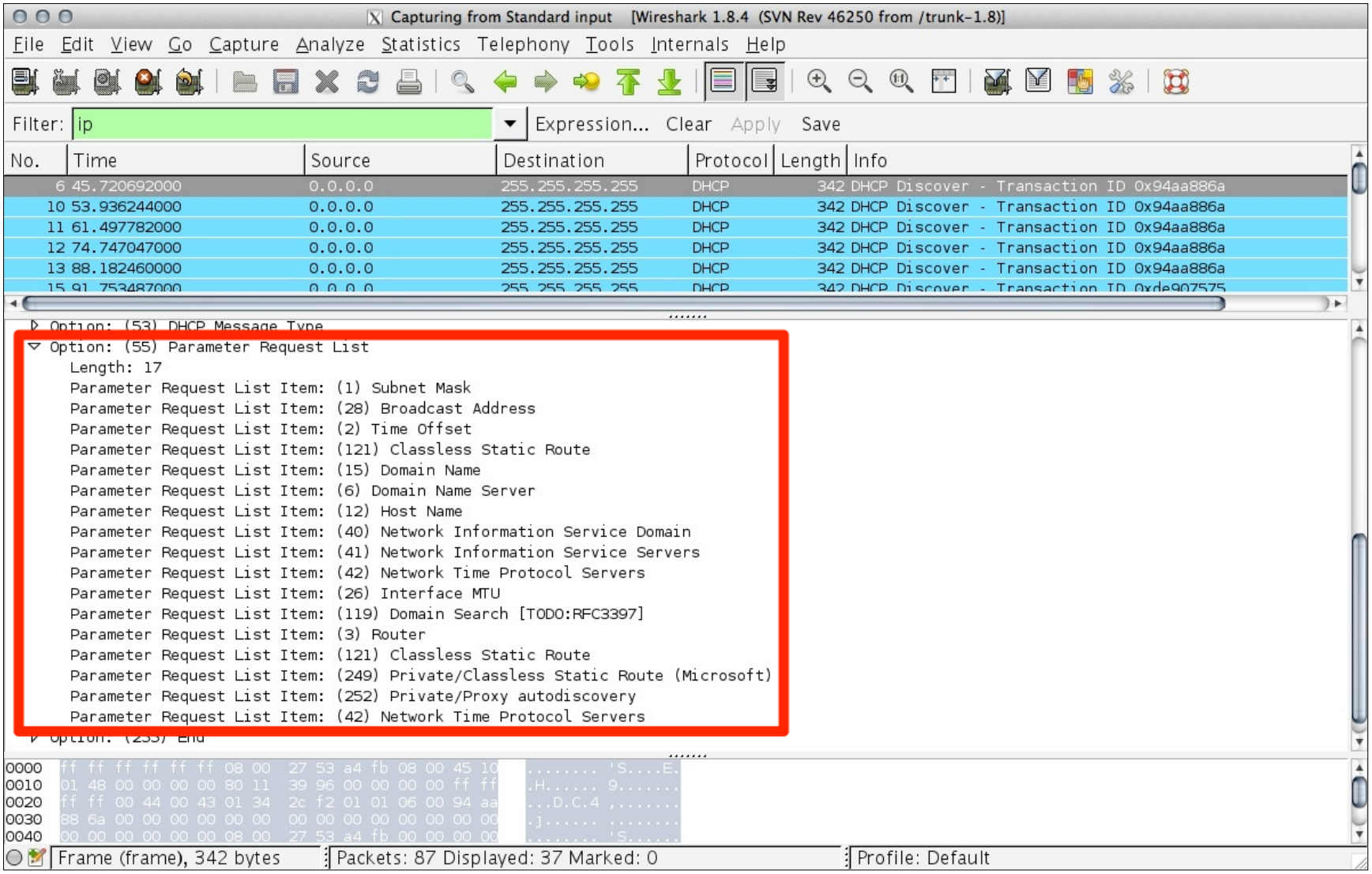
DHCP Fingerprinting



DHCP Fingerprinting

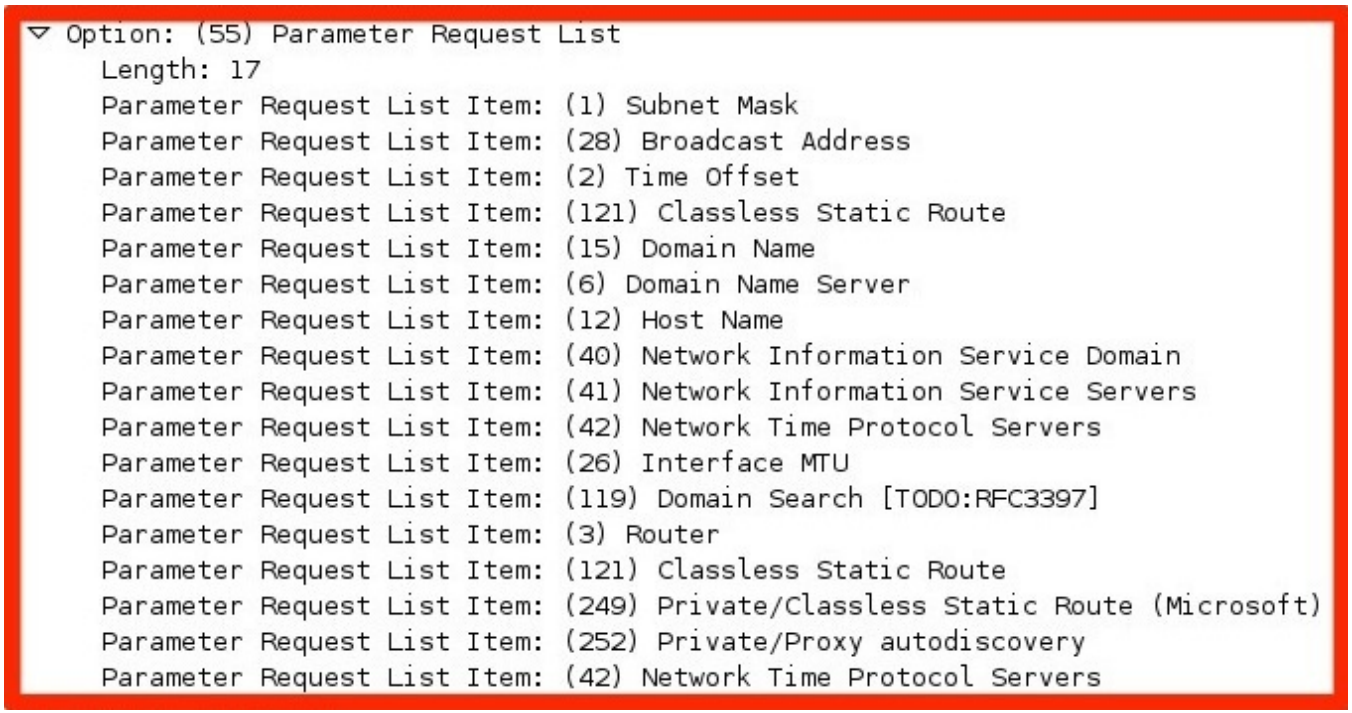


DHCP Fingerprinting



DHCP Fingerprinting

- Option 55: Parameter Request List



1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 121, 249, 252, and 42

DHCP Fingerprint database

- http://www.fingerbank.org

DHCP Fingerprint database

- dhcp_fingerprints.conf (excerpt)

```
858  [os 512]
859  description=Fedora 14 based distro
860  fingerprints=<<EOT
861  1,28,2,121,15,6,12,40,41,42,26,119,3
862  EOT
863
864  [os 513]
865  description=Chrome OS
866  fingerprints=<<EOT
867  1,121,33,3,6,12,15,26,28,51,54,58,59,119
868  EOT
869
870  [os 514]
871  description=Fedora 15 or 16 based distro
872  fingerprints=<<EOT
873  1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42
874  EOT
875
876  [os 515]
877  description=RHEL 6.4 or Centos6.4
878  fingerprints=<<EOT
879  1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,42
880  EOT
881
882  [os 600]
883  description=Xbox
884  fingerprints=<<EOT
885  3,6
886  EOT
```

DHCP Fingerprint database

```
870  [os 514]
871  description=Fedora 15 or 16 based distro
872  fingerprints=<<EOT
873  1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42
874  EOT
```

DHCP Fingerprinting

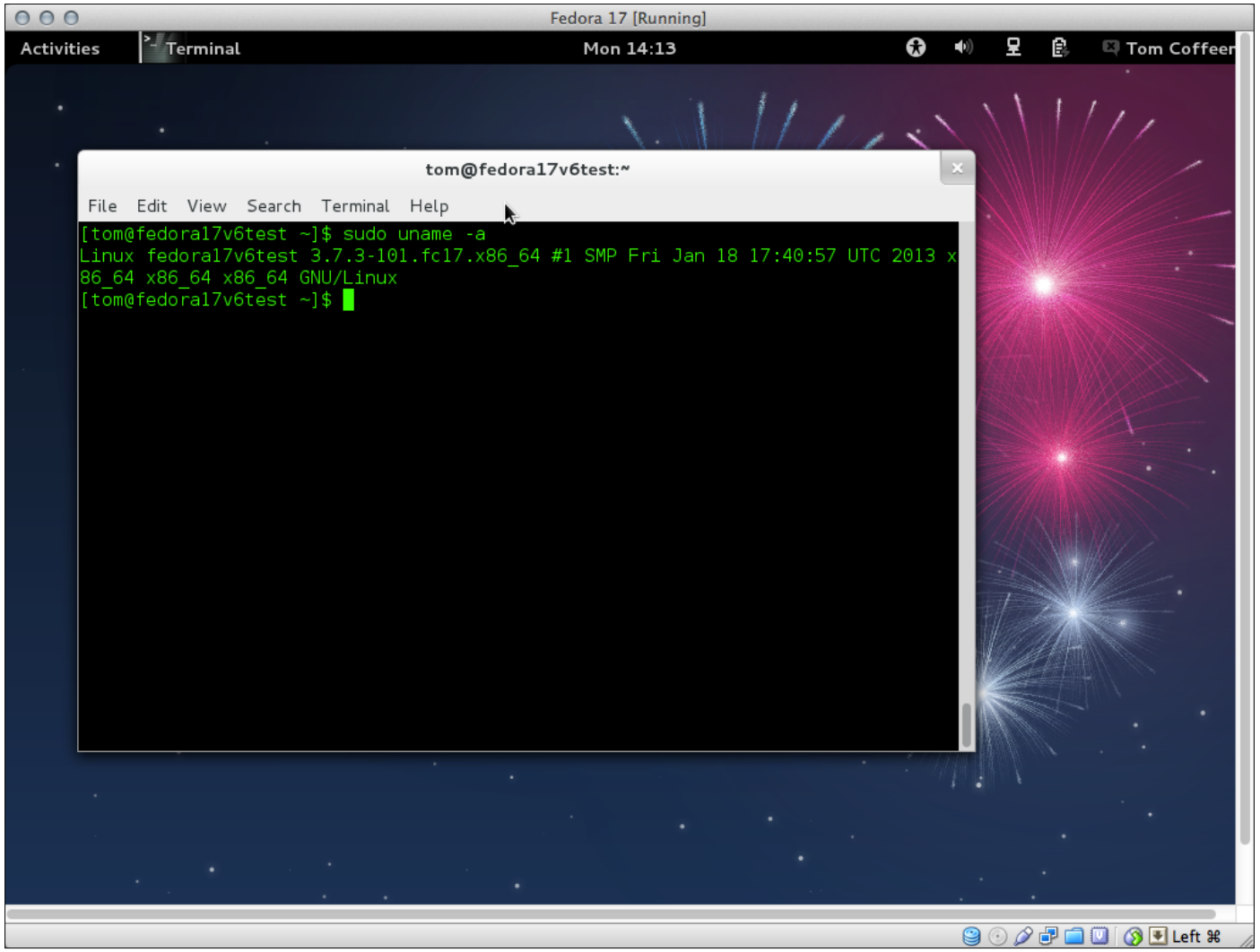
=

Option 55:
1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 121, 249, 252, and 42

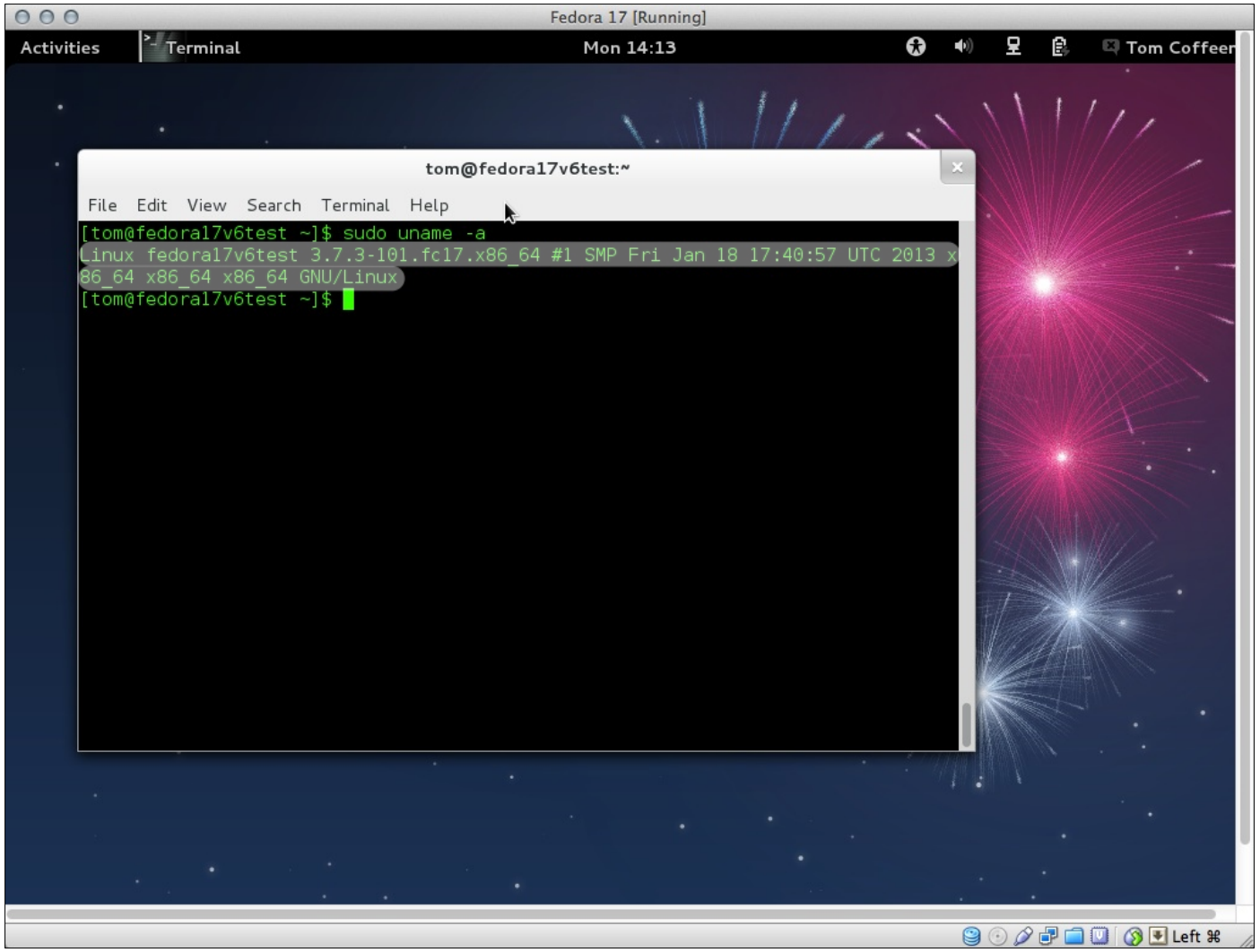
=

Fedora 17

DHCP Fingerprinting



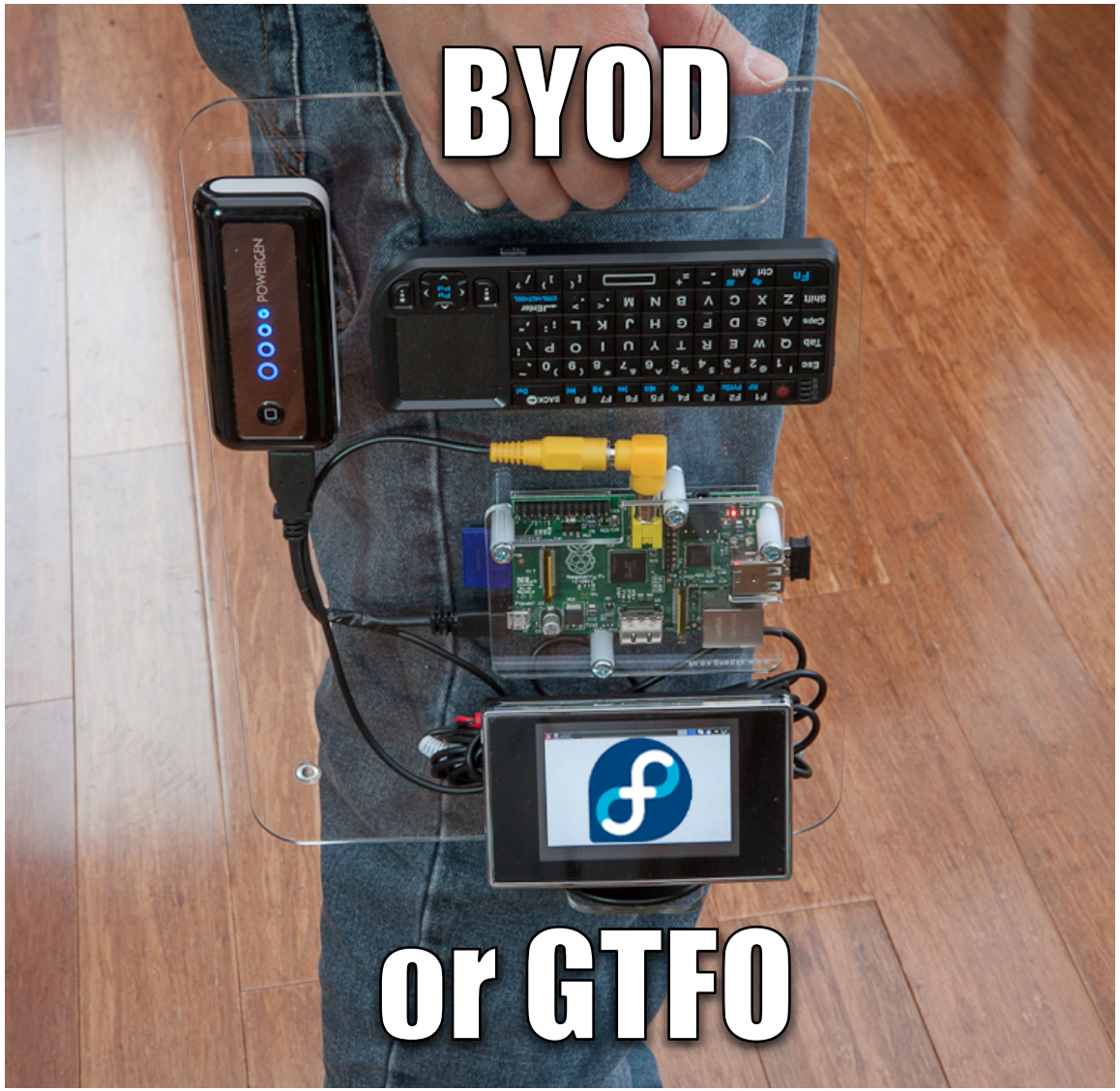
DHCP Fingerprinting



DHCP Fingerprinting

```
Linux fedora17v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x
86_64 x86_64 x86_64 GNU/Linux
```

DHCP Fingerprinting and BYOD



DHCP/DHCPv6 Fingerprinting and BYOD

- Actionable data
  - Security
    - Captive portal approach allows device access or isolation
  - Reporting
    - What devices are connecting (or attempting to connect)?
- Passive -- no additional transactional overhead
  - compare with **nmap** host OS detection

DHCP Fingerprinting and BYOD

- Infoblox HQ BYOD Day
  - Tablets
  - Smartphones
  - Gaming consoles
  - Home routers
  - eReaders
  - Desktops
  - Over 78 unique devices identified
    - Software version learned for 81% of devices

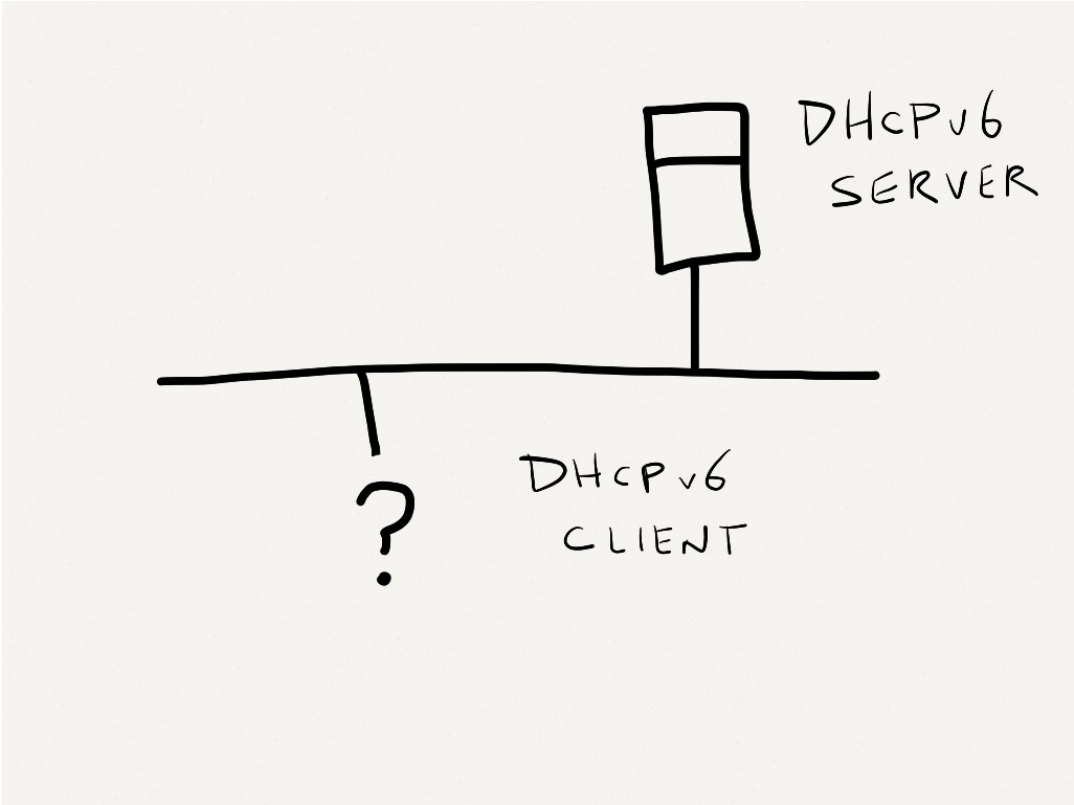
DHCP Fingerprinting

Device	Operating System
Laptop (Window 7)	Professional Service pack 1 Copyright @2009
Apple IPHONE	Version 6.0.1(10A523) Model MD237LL
MAC OS X	Version 10.7.4
MAC OS X	Version 10.5.8
Sony Xperia	AndroidVersion 4.0.4 KernelVersion 2.6.32.9-perf Model MT25I
Samsung Note II	AndroidVersion 4.1.1 KernelVersion 3.031-414933 Model SCH-1605
HTC Android	Version 4.0.4 S/W no - 2.35.531.10710rD HTC Sense Version - 4.1
iTouch	Version 6.1(10B141) Model MD724LL/A
iPhone	Version 6.1(10B143) Model MD638LL/A
iPad 4	Version 6.1(10B141)Â Model MD511LL/A
iPad 2	Version 6.0(10A403)Â Model MD328LL
NOOK Color	Version 1.4.3 Model BNRV200
Kindle	Version 7.2.3_user_2330720
Samsung Galaxy Nexus	Android Version 4.1.1 Kernel Version 3.0.31-g396c4df
ASUS Nexus 7	Android Version 4.2.2 Kernel Version 3.1.10-g05b777c
Apple iPhone 4S	Version 6.1(10B144) Model MC608LL/A
Etc…	

DHCPv6 Fingerprinting

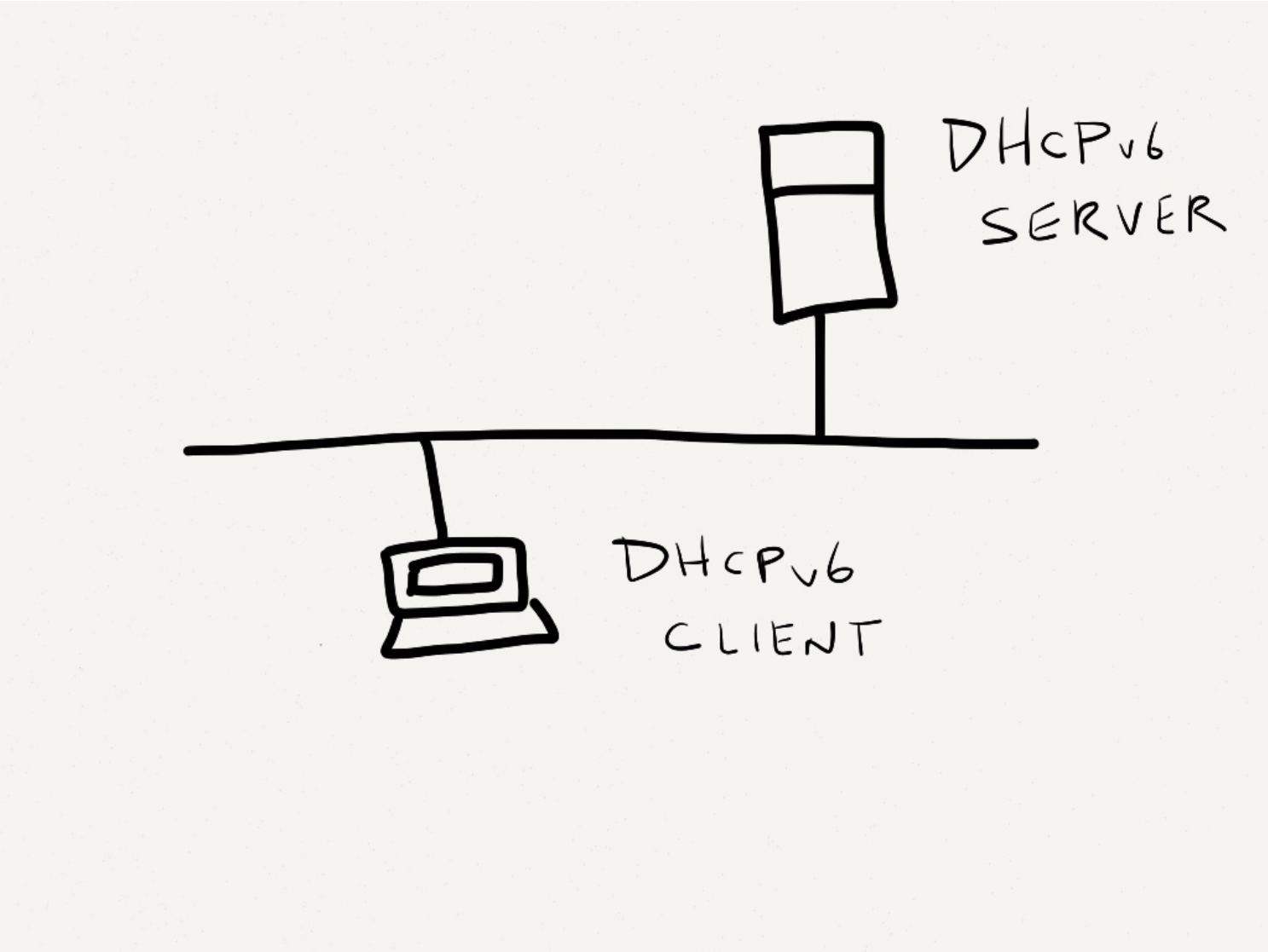
How is DHCPv6 fingerprinting different?

DHCPv6 Fingerprinting

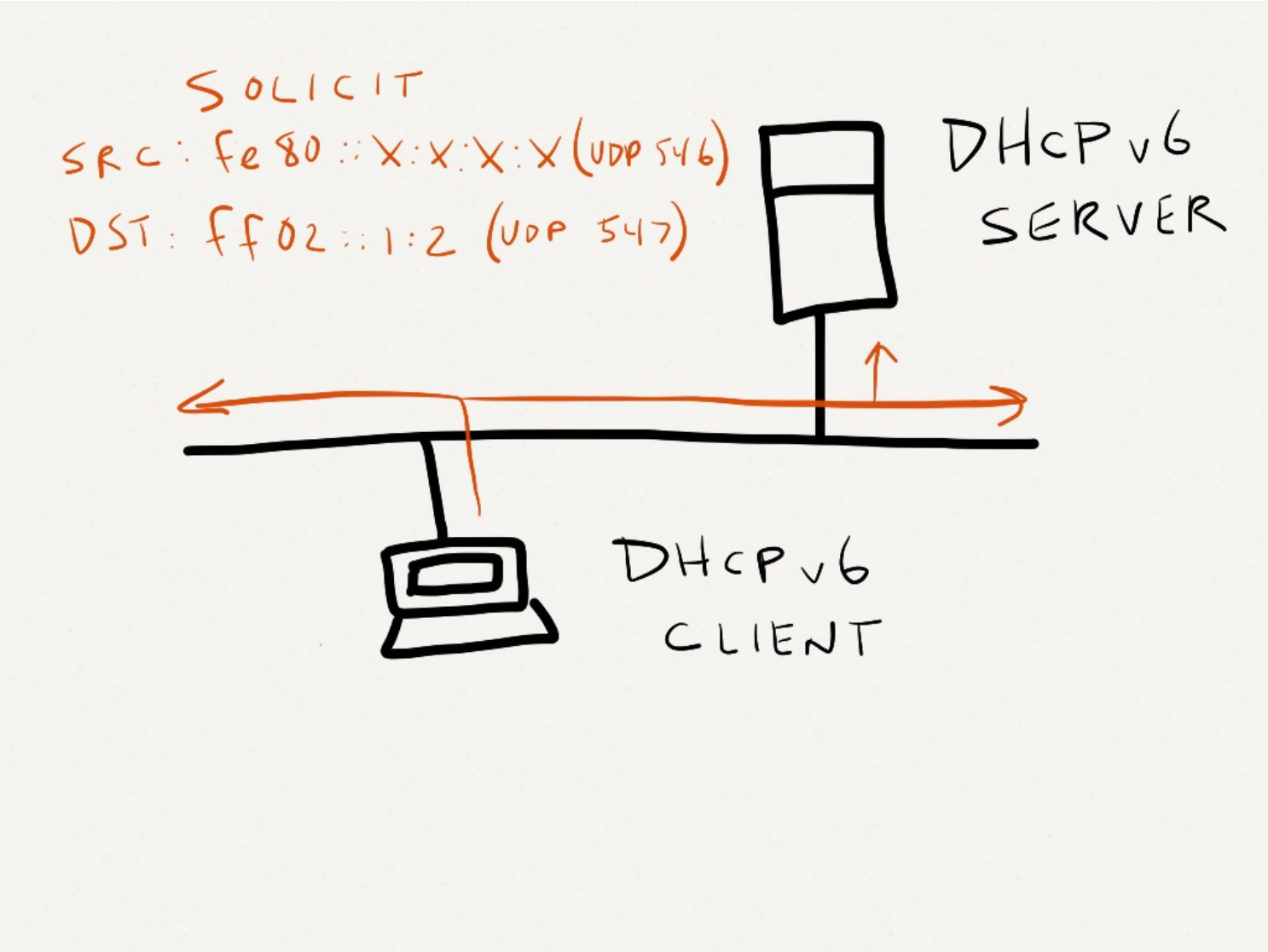


Same goal (client type), this time with DHCPv6

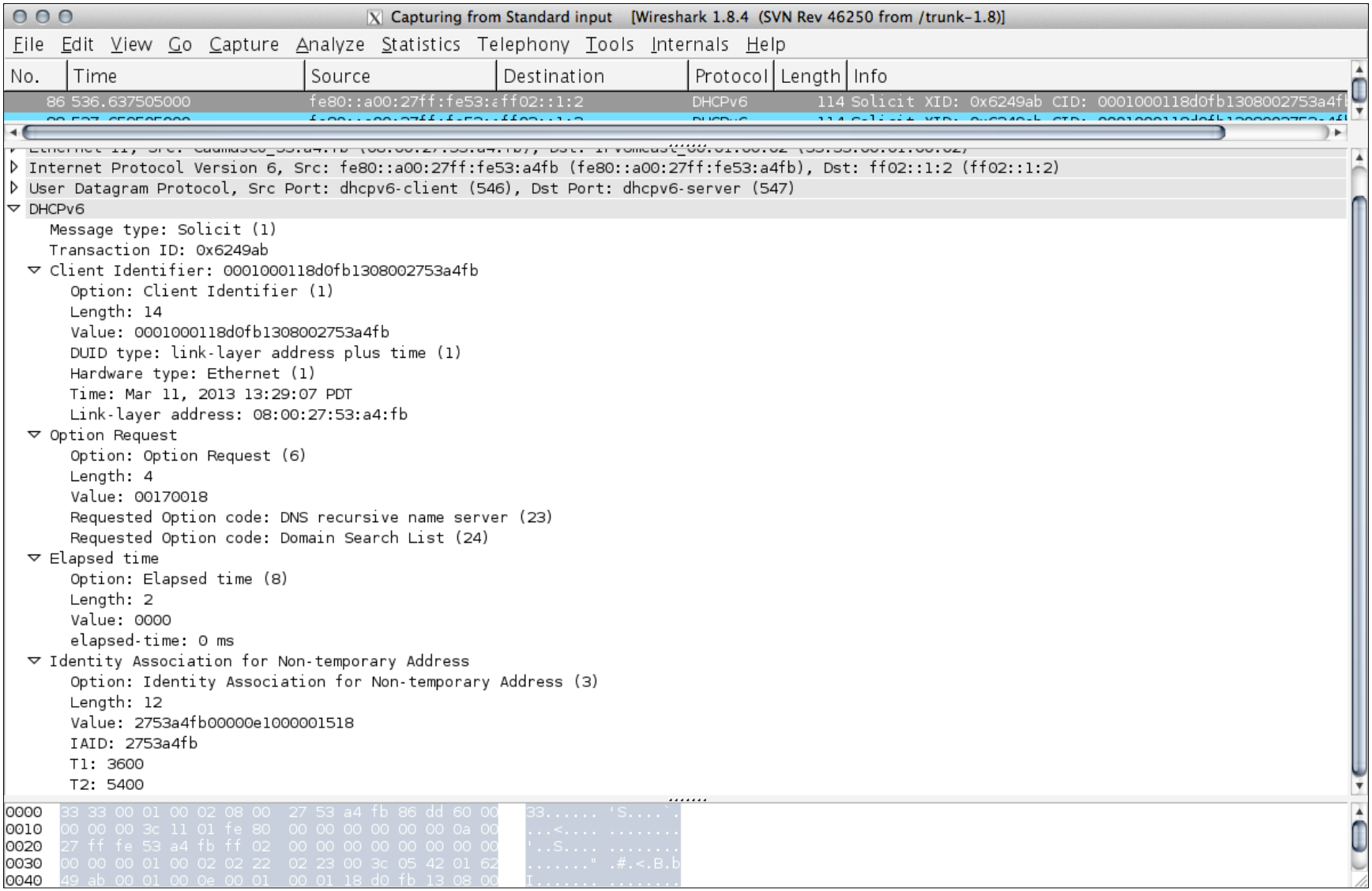
DHCPv6 Fingerprinting



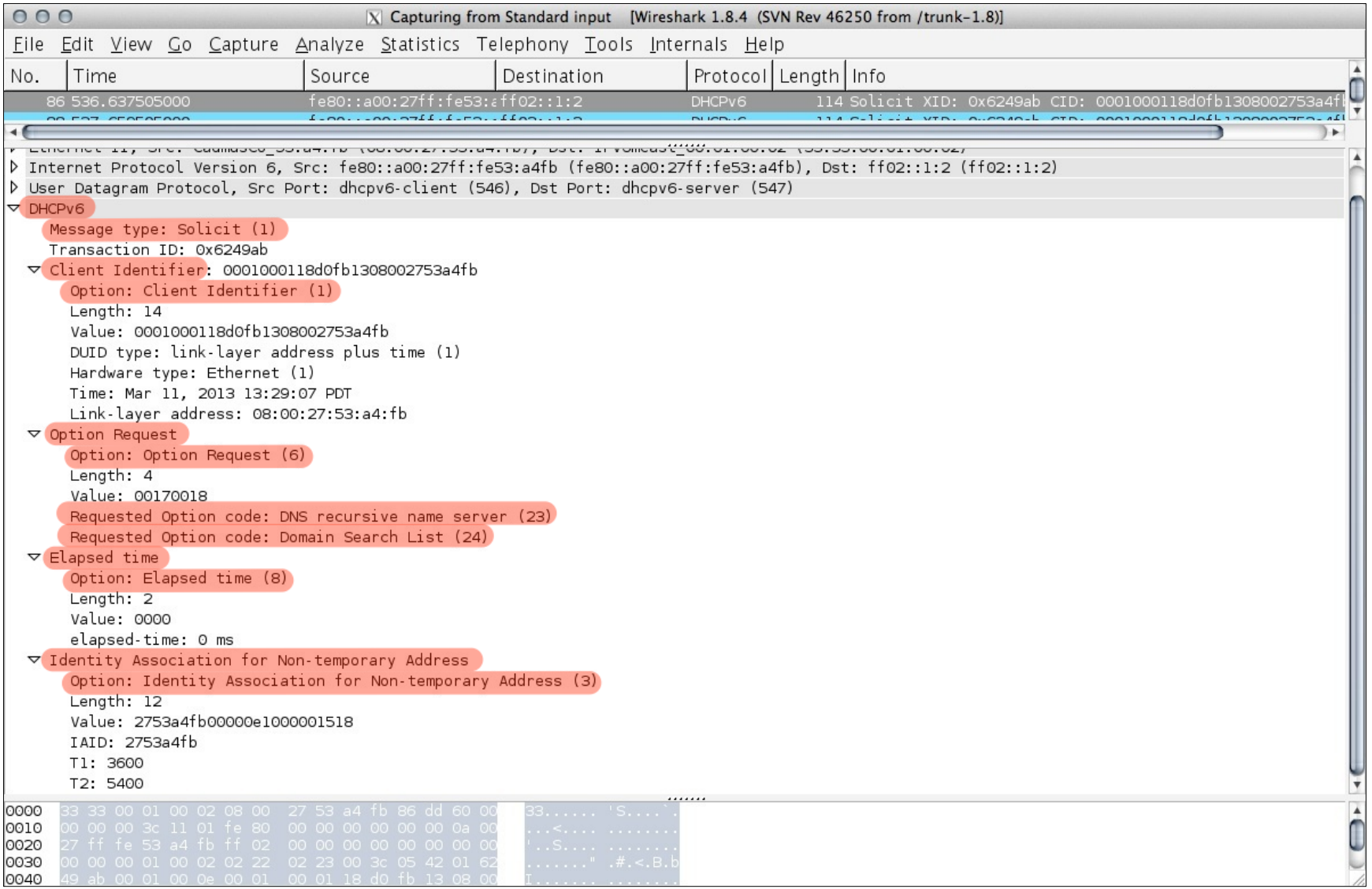
DHCPv6 Fingerprinting



DHCPv6 Fingerprinting



DHCPv6 Fingerprinting



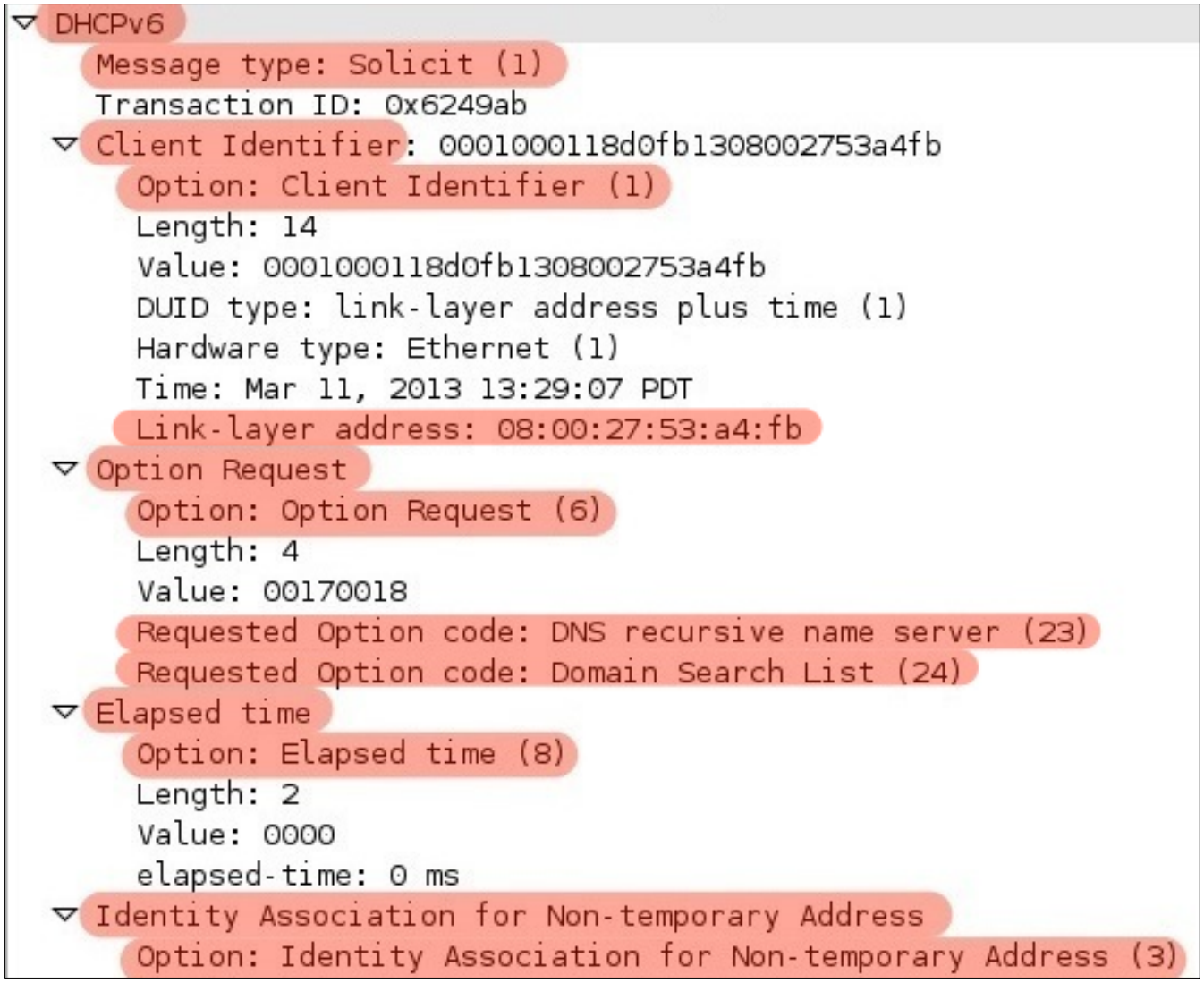
DHCPv6 Fingerprinting

IPv4 DHCP Option Request (Option 55)

DHCPv6 Option Request (Option 6)

- Typically, fewer options appear under Option 6 in a DHCPv6 SOLICIT
- Other elements may be required to validate the device type or system
  - Vendor Class field (where present)
  - Timing how often the client sends a SOLICIT message
  - In dual-stack environments, correlation with the IPv4 fingerprint
  - The Client Identifier field in a DHCPv6 SOLICIT

DHCPv6 Fingerprinting



DHCPv6 Fingerprinting

=

SOLICIT, 1, 6, 23, 24, 8, and 3

=

Fedora 17

DHCPv6 Fingerprints

- Currently, 198 unique fingerprints for DHCP
- None for DHCPv6
  - Likely due to a lack of general IPv6 deployment in environments where fingerprinting is potentially most useful (i.e., enterprise/corporate networks)
  - Thus, BYOD not generally a challenge for IPv6 (*yet*…)

DHCPv6 Fingerprints

- Collaborating with UNH-IOL on a public DHCPv6 fingerprint database
  - Benefits
    - IPv6 feature parity for a durably useful feature in IPv4
    - Increases the likelihood that the greatest number of devices will be accurately identified over time
    - May encourage the deployment of DHCPv6
    - May encourage effective BYOD policy

Infoblox
CONTROL YOUR NETWORK

Questions?

tcoffeen@infoblox.com

twitter: @ipv6tom

References

- 2012 Internet Trends, Mary Meeker (KPCB), Dec. 2012
  - http://www.kpcb.com/insights/2012-internet-trends
- IPv4 Address Report, Geoff Huston (APNIC), Mar. 2013
  - http://www.potaroo.net/tools/ipv4/
- Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, IETF, Jul. 2003
- Dynamic Host Configuration Protocol, RFC 2131, IETF, Mar. 1997
- Chatter on the Wire: A look at DHCPv6 traffic, by Eric Kollmann, Nov. 2010
  - http://chatteronthewire.org/download/chatter-dhcpv6.pdf