Infoblox®
CONTROL YOUR NETWORK

DHCPv6 Fingerprinting and BYOD

Tom Coffeen, IPv6 Evangelist

NAv6TF Summit 2013

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:

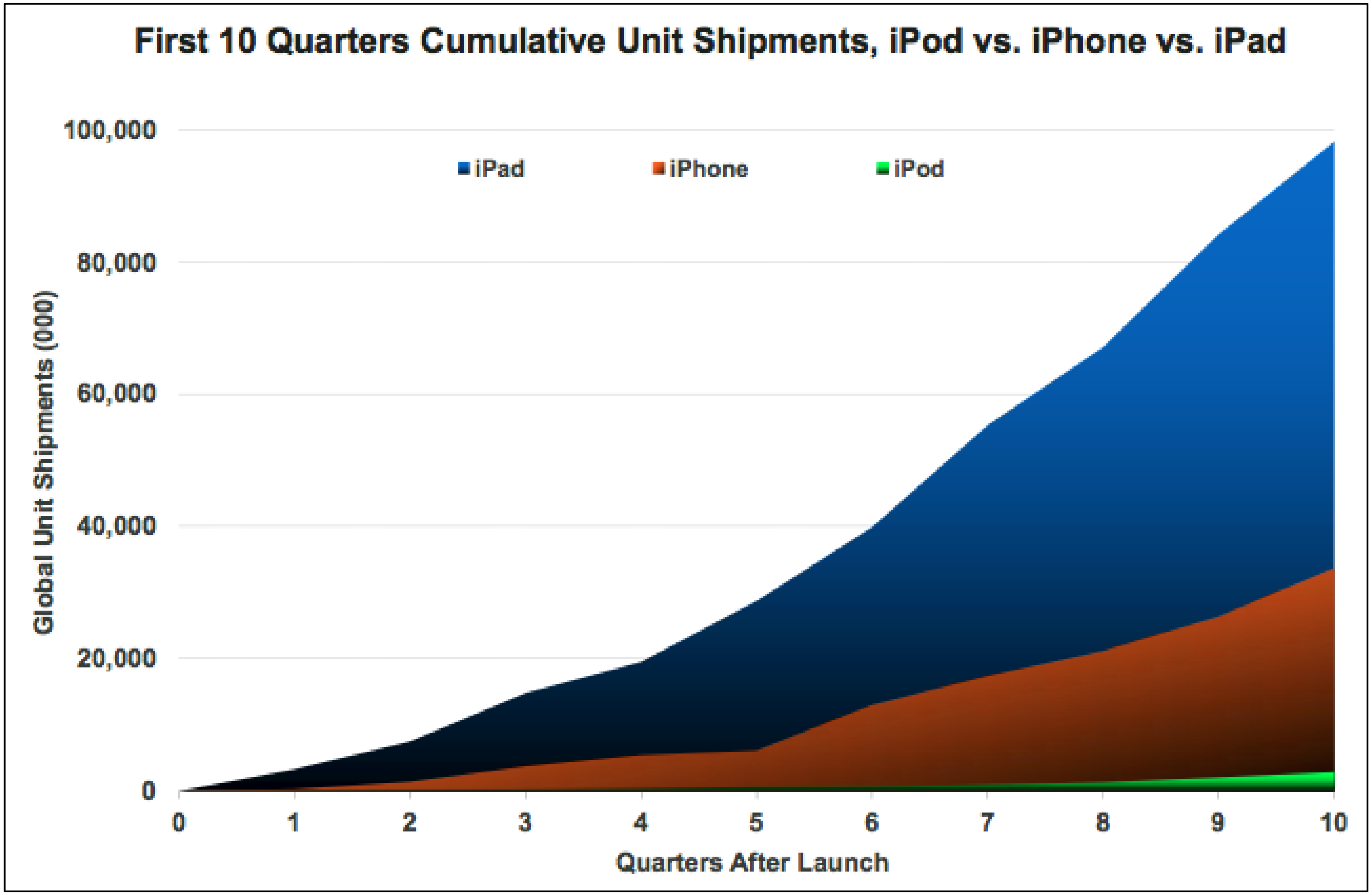
a) The latest hip hop sensation from Slovenia (no cheating by asking Jan Z!)

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

c) Line four on the eye chart

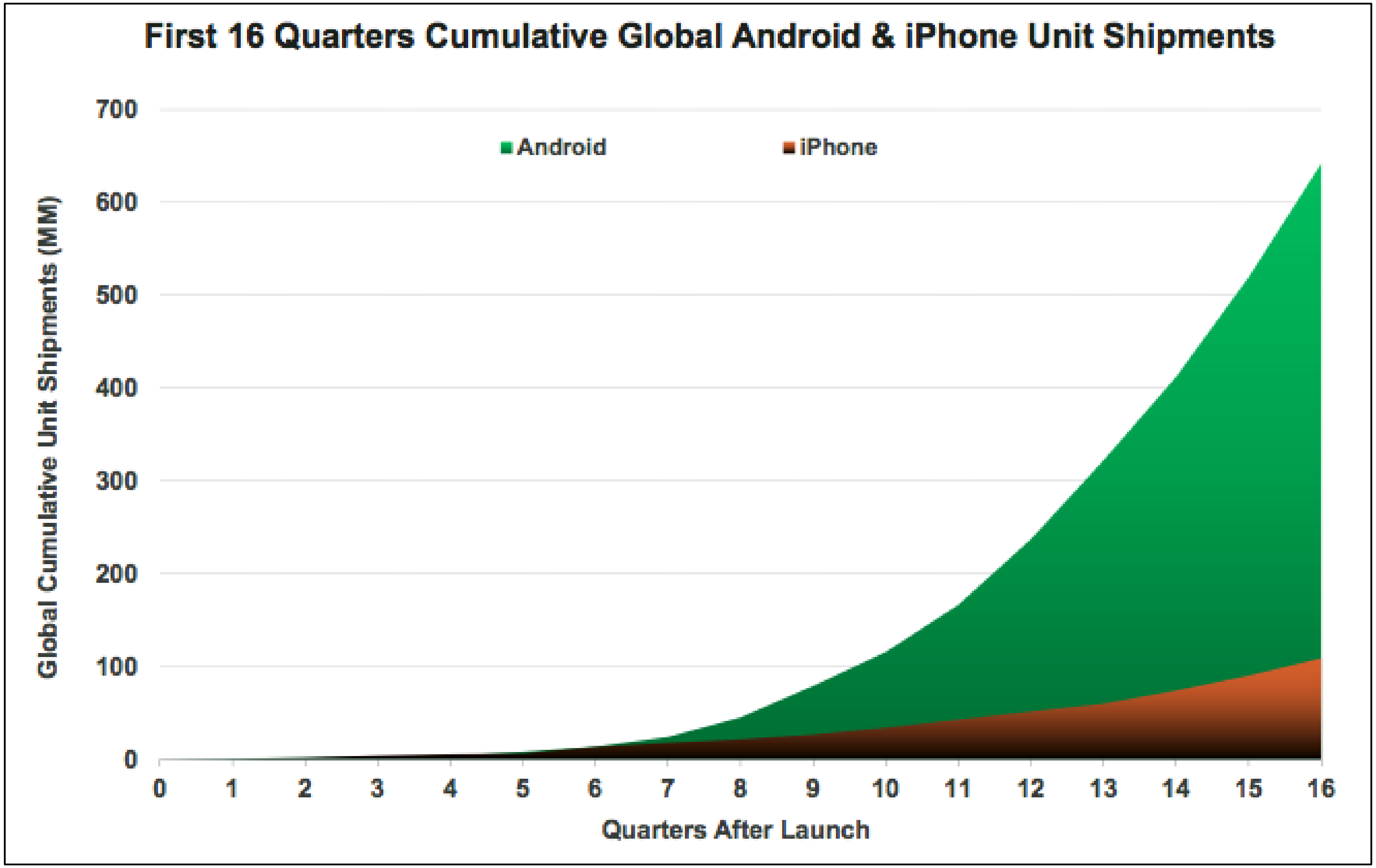
d) An abbreviation for "bring your own device"; i.e., end user personal devices on the corporate network

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



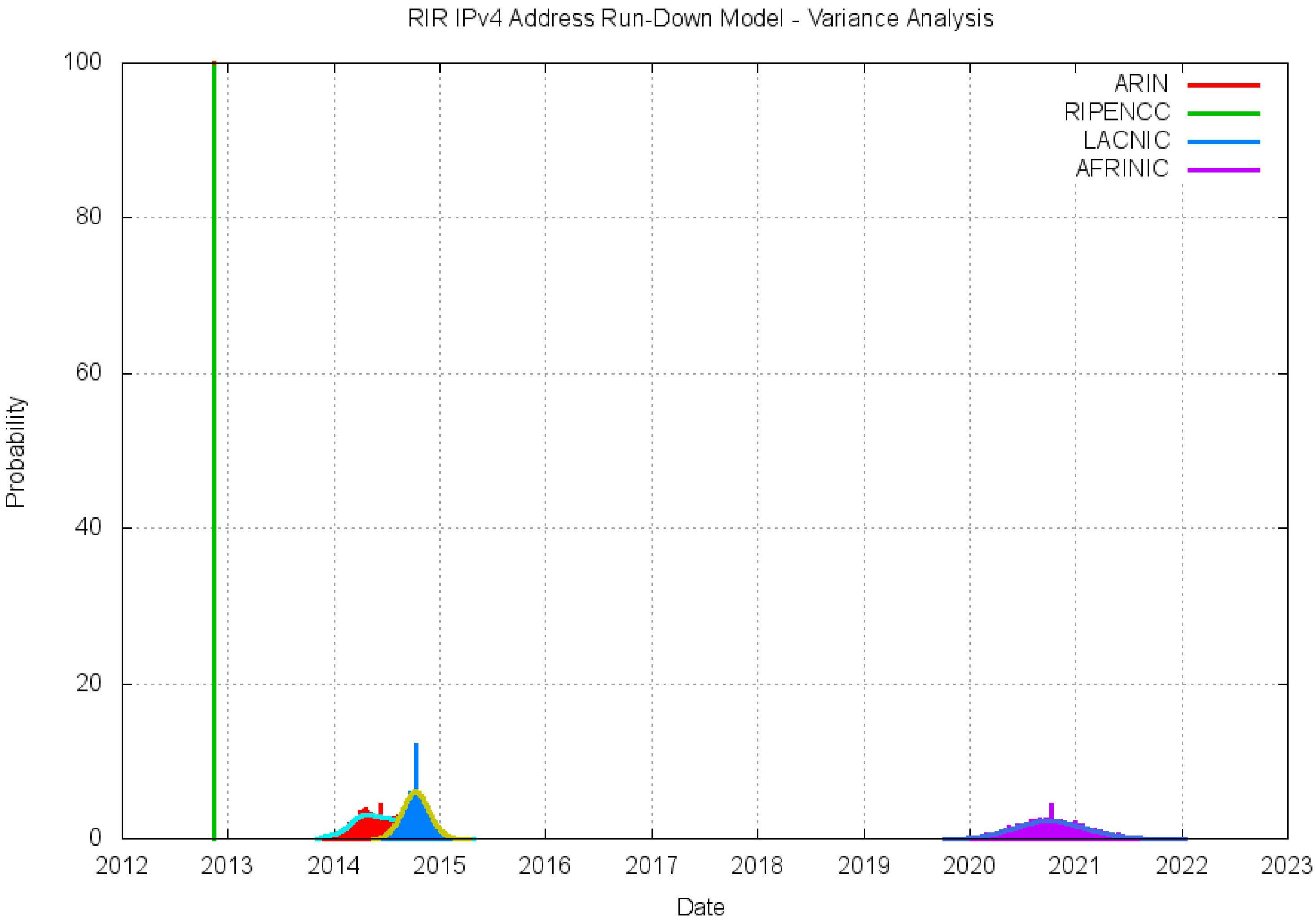
Source: Mary Meeker, Internet Trends @Stanford – Bases 12/03/2012

Infoblox

This slide is awesome

4,294,967,296 < 7,000,000,000

And why the BYOD challenge will include IPv6

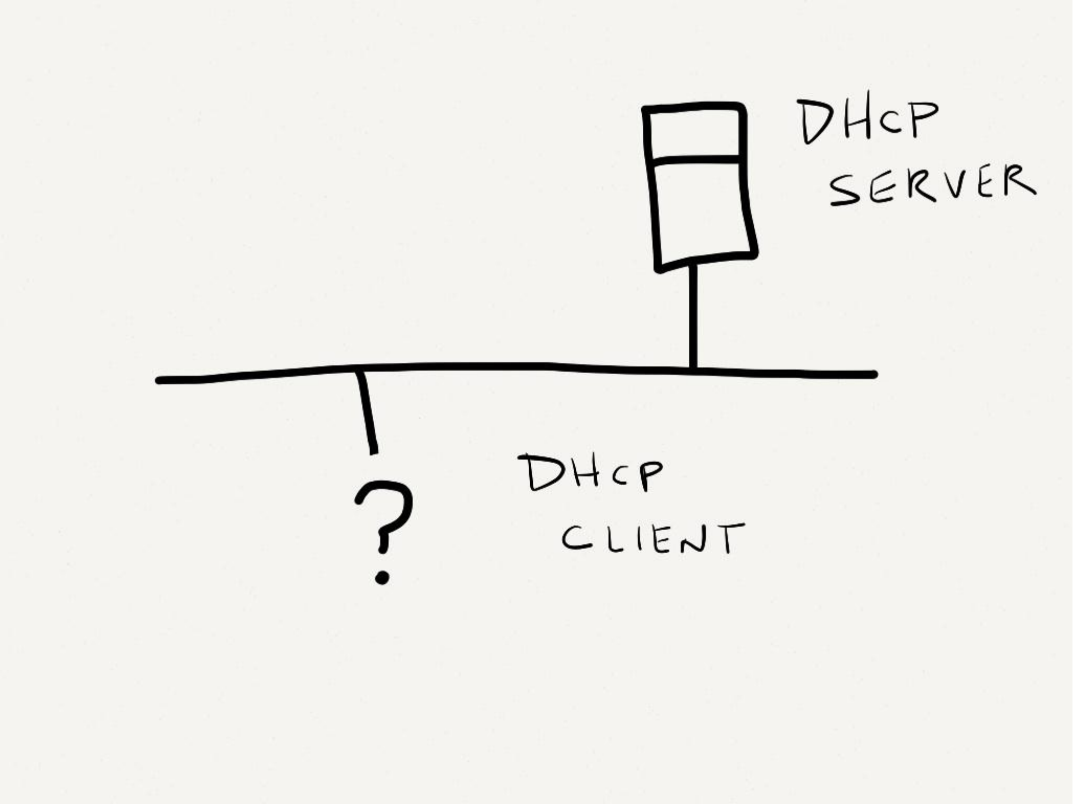


Source: Geoff Huston IPv4 Address Report, 4/8/2013

DHCP(v6) Fingerprinting

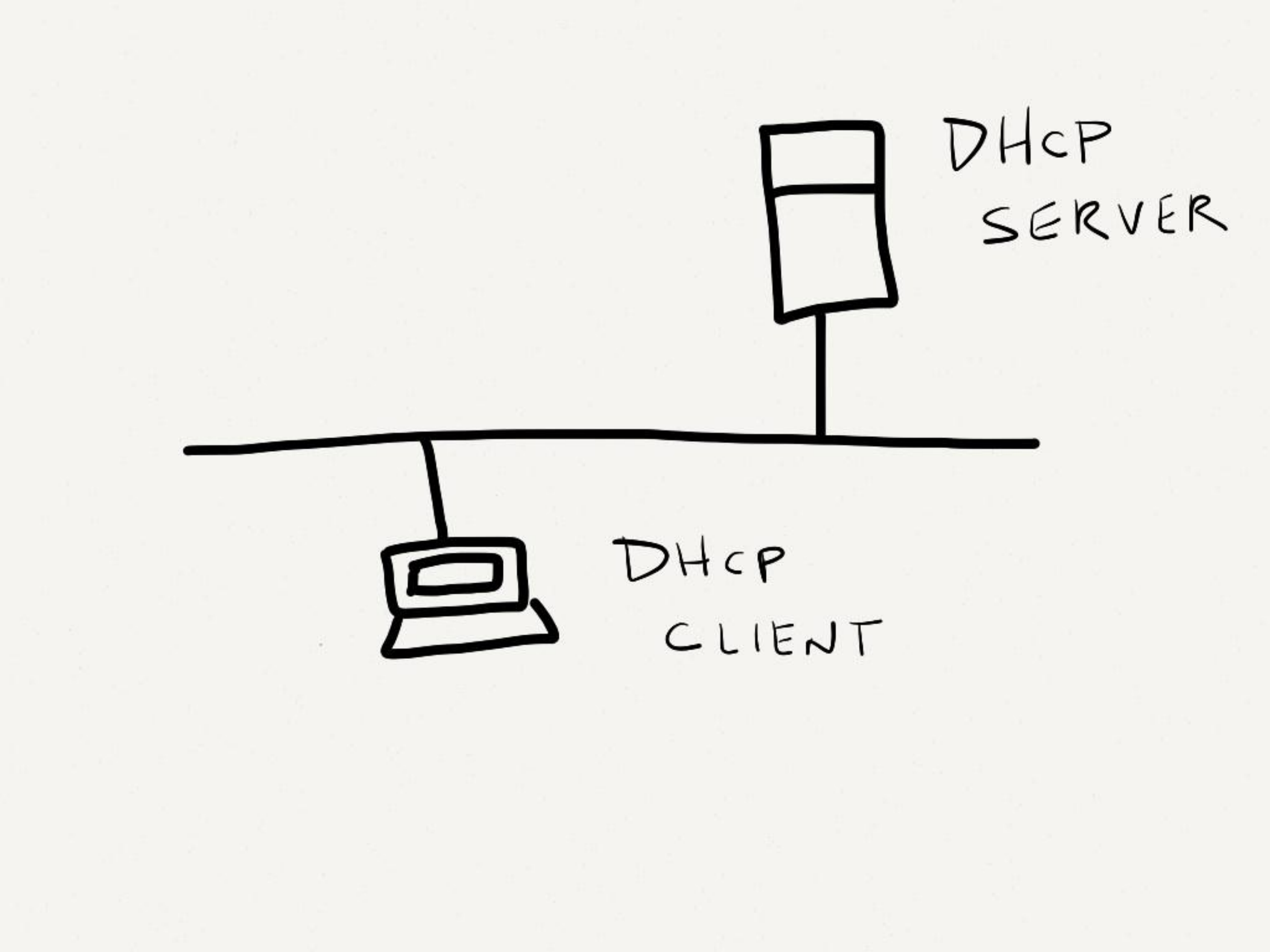
What is DHCP(v6) fingerprinting?

DHCP Fingerprinting

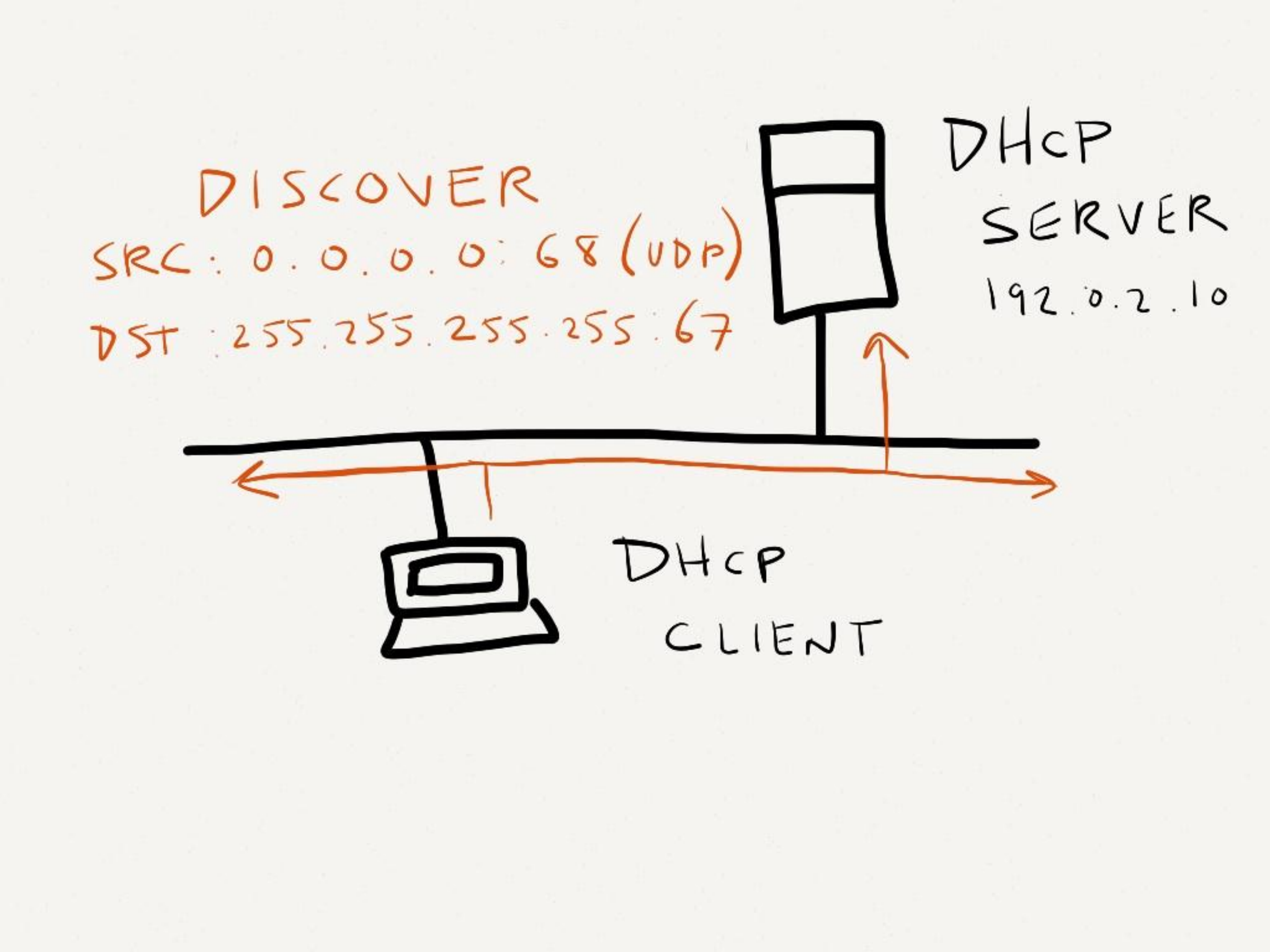


The goal is to determine the client type using only data from a basic DHCP transaction

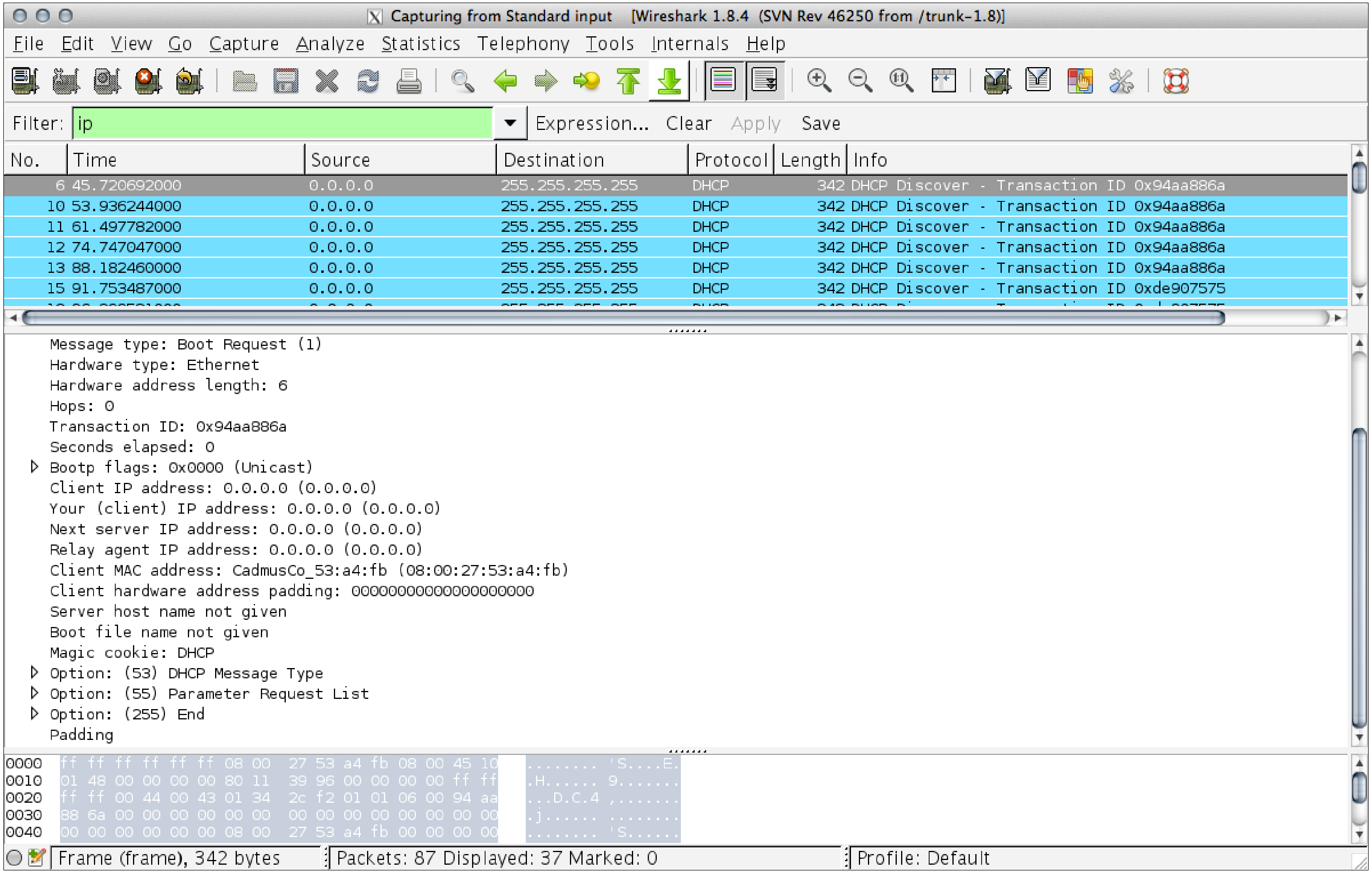
DHCP Transaction



DHCP Transaction



DHCP Fingerprinting



Capturing from Standard input [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip

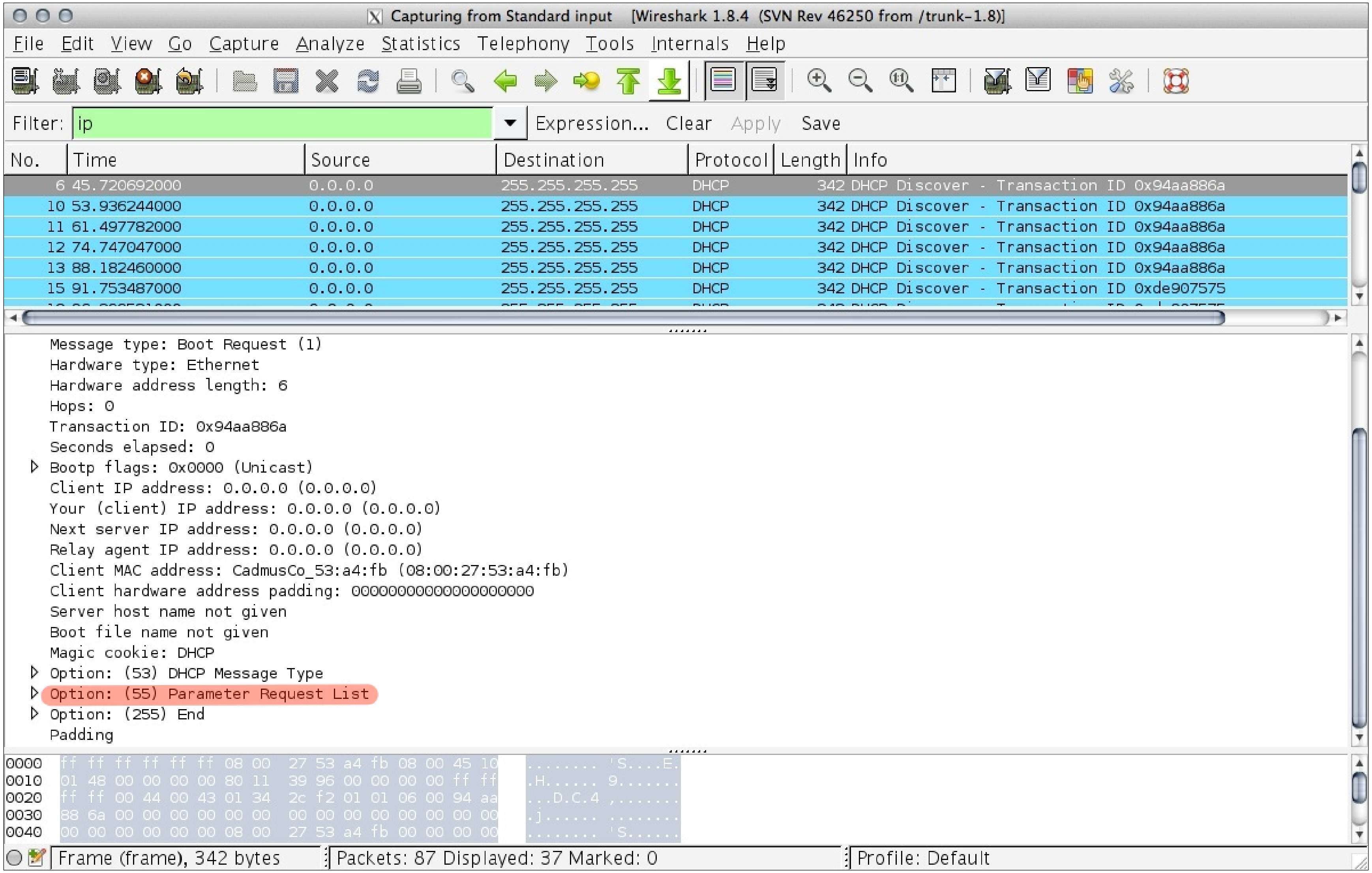
```
No.  Time            Source    Destination      Protocol  Length  Info
   6 45.720692000    0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x94aa886a
  10 53.936244000    0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x94aa886a
  11 61.497782000    0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x94aa886a
  12 74.747047000    0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x94aa886a
  13 88.182460000    0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x94aa886a
  15 91.753487000    0.0.0.0   255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0xde907575
```

```
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x94aa886a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: CadmusCo_53:a4:fb (08:00:27:53:a4:fb)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▷ Option: (53) DHCP Message Type
  ▷ Option: (55) Parameter Request List
  ▷ Option: (255) End
    Padding
```

```
0000  ff ff ff ff ff ff 08 00  27 53 a4 fb 08 00 45 10   ........ 'S....E.
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   .H...... 9.......
0020  ff ff 00 44 00 43 01 34  2c f2 01 01 06 00 94 aa   ...D.C.4 ,.......
0030  88 6a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .j...... ........
0040  00 00 00 00 00 00 08 00  27 53 a4 fb 00 00 00 00   ........ 'S......
```

Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default

DHCP Fingerprinting


Capturing from Standard input [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip

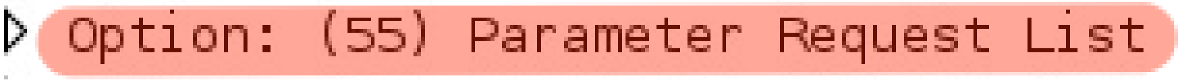
```
No.  Time            Source     Destination       Protocol Length Info
   6 45.720692000   0.0.0.0    255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x94aa886a
  10 53.936244000   0.0.0.0    255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x94aa886a
  11 61.497782000   0.0.0.0    255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x94aa886a
  12 74.747047000   0.0.0.0    255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x94aa886a
  13 88.182460000   0.0.0.0    255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x94aa886a
  15 91.753487000   0.0.0.0    255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0xde907575
```

```
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x94aa886a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: CadmusCo_53:a4:fb (08:00:27:53:a4:fb)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▷ Option: (53) DHCP Message Type
  ▷ Option: (55) Parameter Request List
  ▷ Option: (255) End
    Padding
```

```
0000  ff ff ff ff ff ff 08 00  27 53 a4 fb 08 00 45 10   ........ 'S....E.
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   .H...... 9.......
0020  ff ff 00 44 00 43 01 34  2c f2 01 01 06 00 94 aa   ...D.C.4 ,.......
0030  88 6a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .j...... ........
0040  00 00 00 00 00 00 08 00  27 53 a4 fb 00 00 00 00   ........ 'S......
```

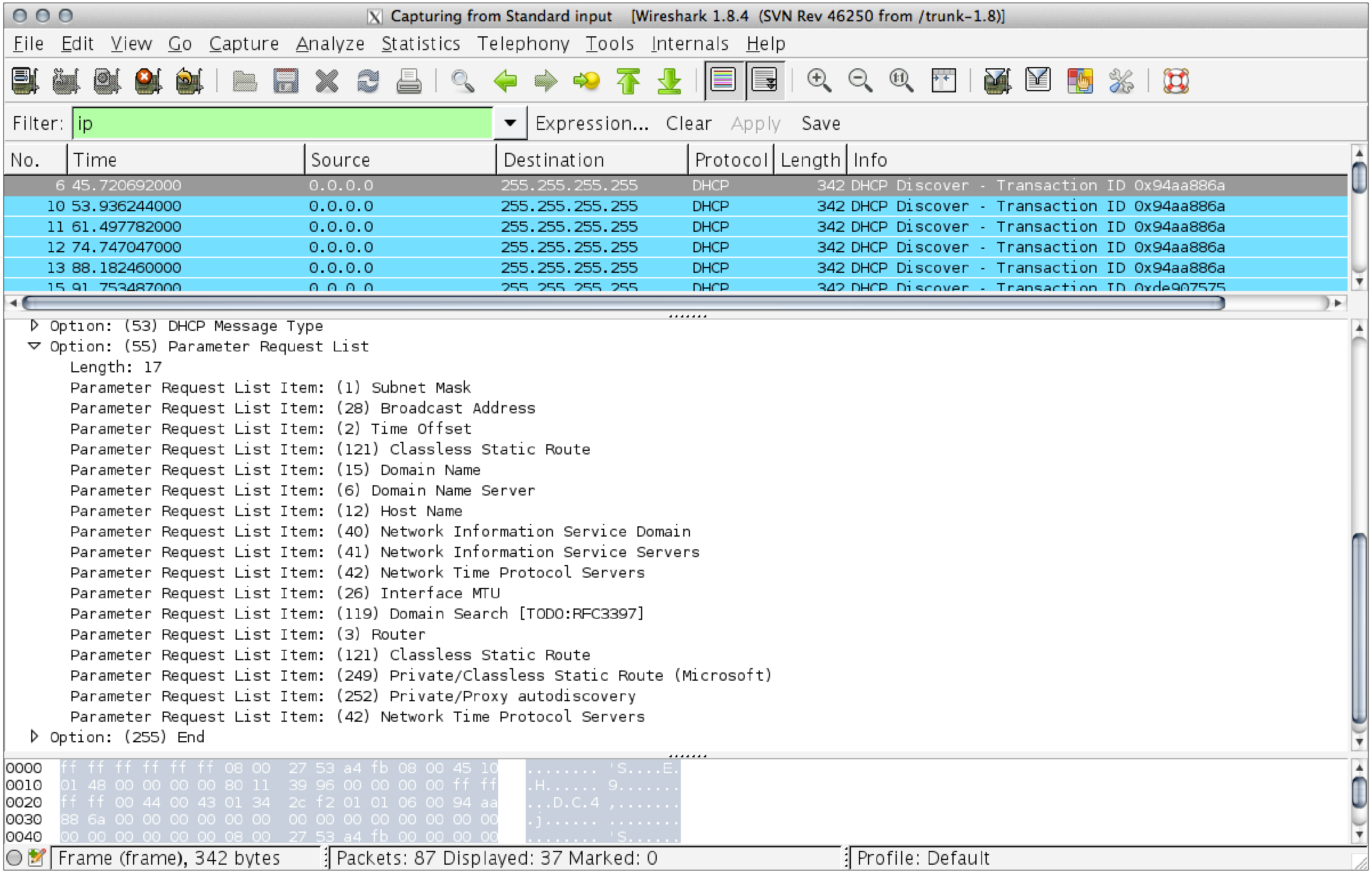
Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default

DHCP Fingerprinting



```
▷ Option: (55) Parameter Request List
```

DHCP Fingerprinting



Capturing from Standard input [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip

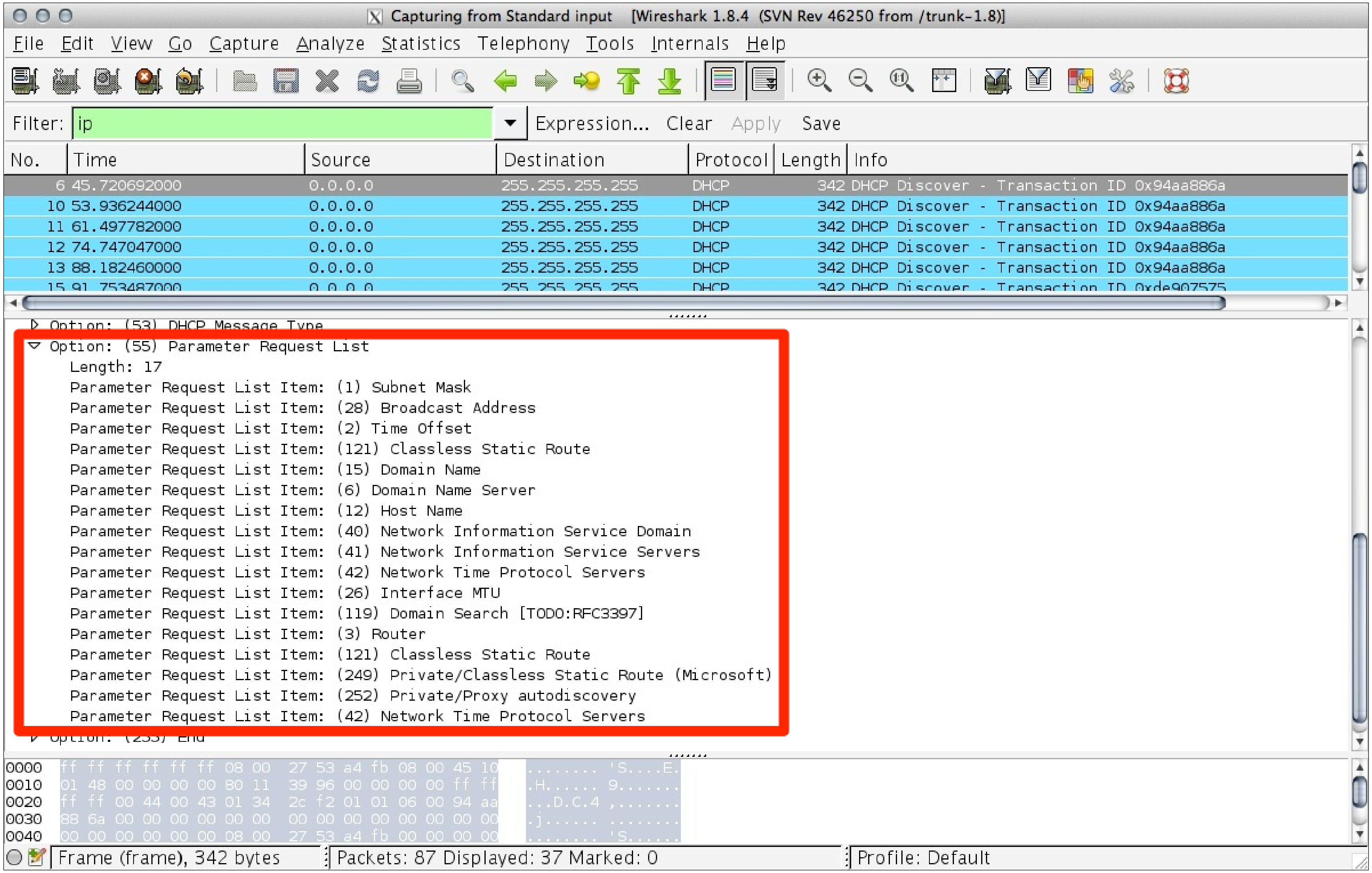
```
No.  Time          Source     Destination       Protocol Length Info
   6 45.720692000  0.0.0.0    255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x94aa886a
  10 53.936244000  0.0.0.0    255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x94aa886a
  11 61.497782000  0.0.0.0    255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x94aa886a
  12 74.747047000  0.0.0.0    255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x94aa886a
  13 88.182460000  0.0.0.0    255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0x94aa886a
  15 91.753487000  0.0.0.0    255.255.255.255   DHCP        342 DHCP Discover - Transaction ID 0xde907575
```

```
▷ Option: (53) DHCP Message Type
▽ Option: (55) Parameter Request List
    Length: 17
    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: (121) Classless Static Route
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (40) Network Information Service Domain
    Parameter Request List Item: (41) Network Information Service Servers
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (119) Domain Search [TODO:RFC3397]
    Parameter Request List Item: (3) Router
    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
    Parameter Request List Item: (42) Network Time Protocol Servers
▷ Option: (255) End
```

```
0000  ff ff ff ff ff ff 08 00  27 53 a4 fb 08 00 45 10   ........ 'S....E.
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   .H...... 9.......
0020  ff ff 00 44 00 43 01 34  2c f2 01 01 06 00 94 aa   ...D.C.4 ,.......
0030  88 6a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .j...... ........
0040  00 00 00 00 00 00 08 00  27 53 a4 fb 00 00 00 00   ........ 'S......
```

Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default

DHCP Fingerprinting



Capturing from Standard input [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: ip

```
No.  Time                 Source      Destination        Protocol  Length  Info
   6 45.720692000         0.0.0.0     255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x94aa886a
  10 53.936244000         0.0.0.0     255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x94aa886a
  11 61.497782000         0.0.0.0     255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x94aa886a
  12 74.747047000         0.0.0.0     255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x94aa886a
  13 88.182460000         0.0.0.0     255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x94aa886a
  15 91.753487000         0.0.0.0     255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0xde907575
```

```
▷ Option: (53) DHCP Message Type
▽ Option: (55) Parameter Request List
    Length: 17
    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: (121) Classless Static Route
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (40) Network Information Service Domain
    Parameter Request List Item: (41) Network Information Service Servers
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (119) Domain Search [TODO:RFC3397]
    Parameter Request List Item: (3) Router
    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
    Parameter Request List Item: (42) Network Time Protocol Servers
▷ Option: (255) End
```

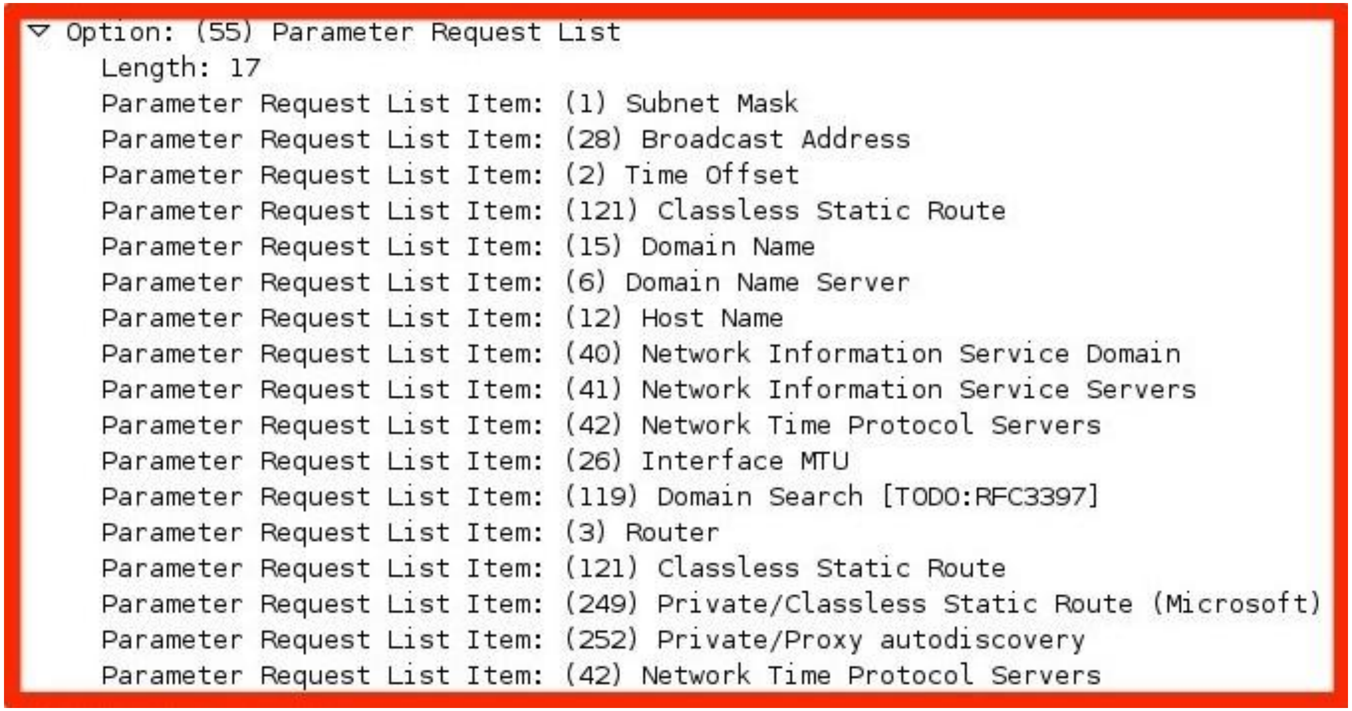
```
0000  ff ff ff ff ff ff 08 00  27 53 a4 fb 08 00 45 10   ........ 'S....E.
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   .H...... 9.......
0020  ff ff 00 44 00 43 01 34  2c f2 01 01 06 00 94 aa   ...D.C.4 ,.......
0030  88 6a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .j...... ........
0040  00 00 00 00 00 00 08 00  27 53 a4 fb 00 00 00 00   ........ 'S......
```

Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default

Infoblox

DHCP Fingerprinting

- Option 55: Parameter Request List



```
▽ Option: (55) Parameter Request List
    Length: 17
    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: (121) Classless Static Route
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (40) Network Information Service Domain
    Parameter Request List Item: (41) Network Information Service Servers
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (119) Domain Search [TODO:RFC3397]
    Parameter Request List Item: (3) Router
    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
    Parameter Request List Item: (42) Network Time Protocol Servers
```

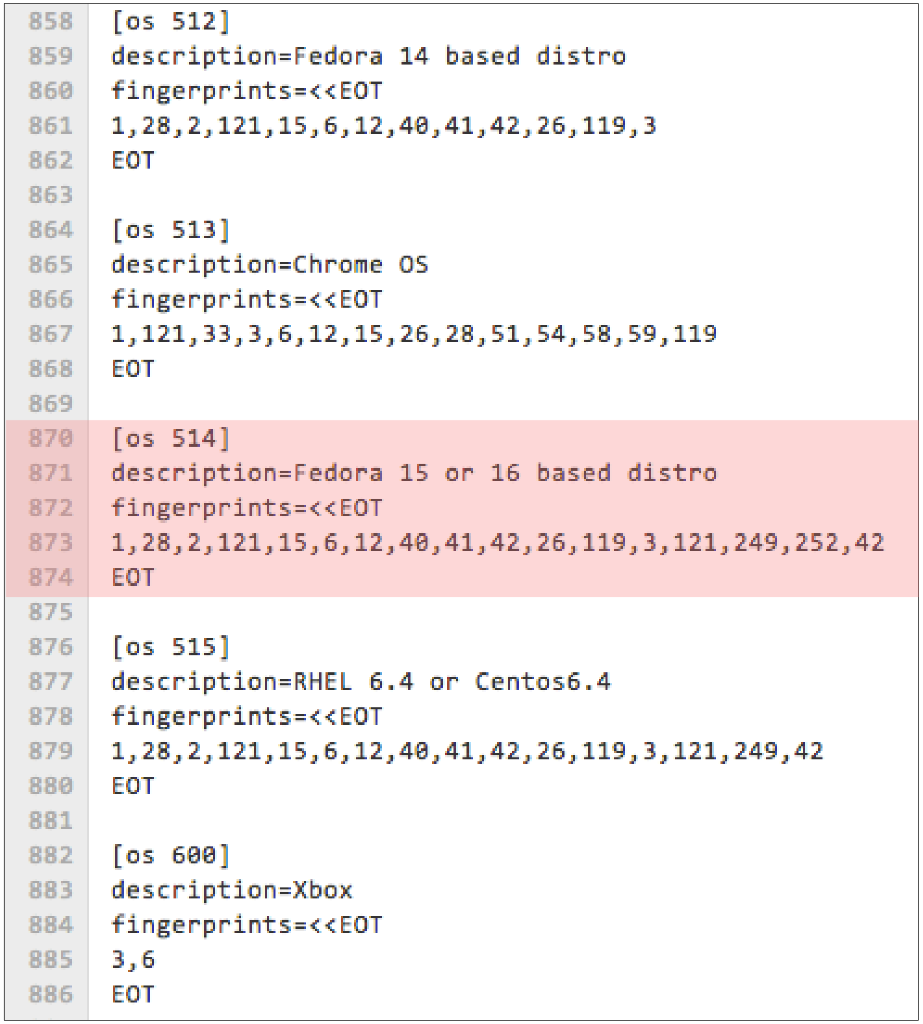
1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 121, 249, 252, and 42

DHCP Fingerprint database

- http://www.fingerbank.org

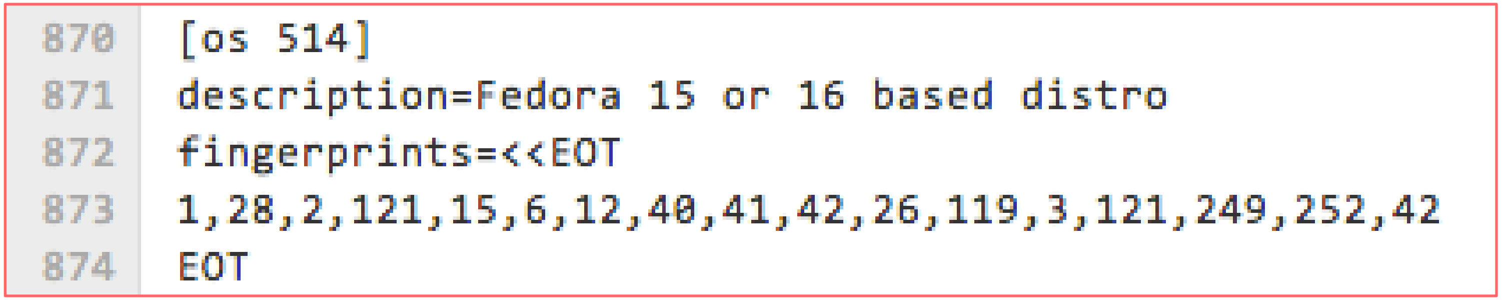
DHCP Fingerprint database

- dhcp_fingerprints.conf (excerpt)



```
[os 512]
description=Fedora 14 based distro
fingerprints=<<EOT
1,28,2,121,15,6,12,40,41,42,26,119,3
EOT

[os 513]
description=Chrome OS
fingerprints=<<EOT
1,121,33,3,6,12,15,26,28,51,54,58,59,119
EOT

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

[os 515]
description=RHEL 6.4 or Centos6.4
fingerprints=<<EOT
1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,42
EOT

[os 600]
description=Xbox
fingerprints=<<EOT
3,6
EOT
```

DHCP Fingerprint database



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

DHCP Fingerprinting

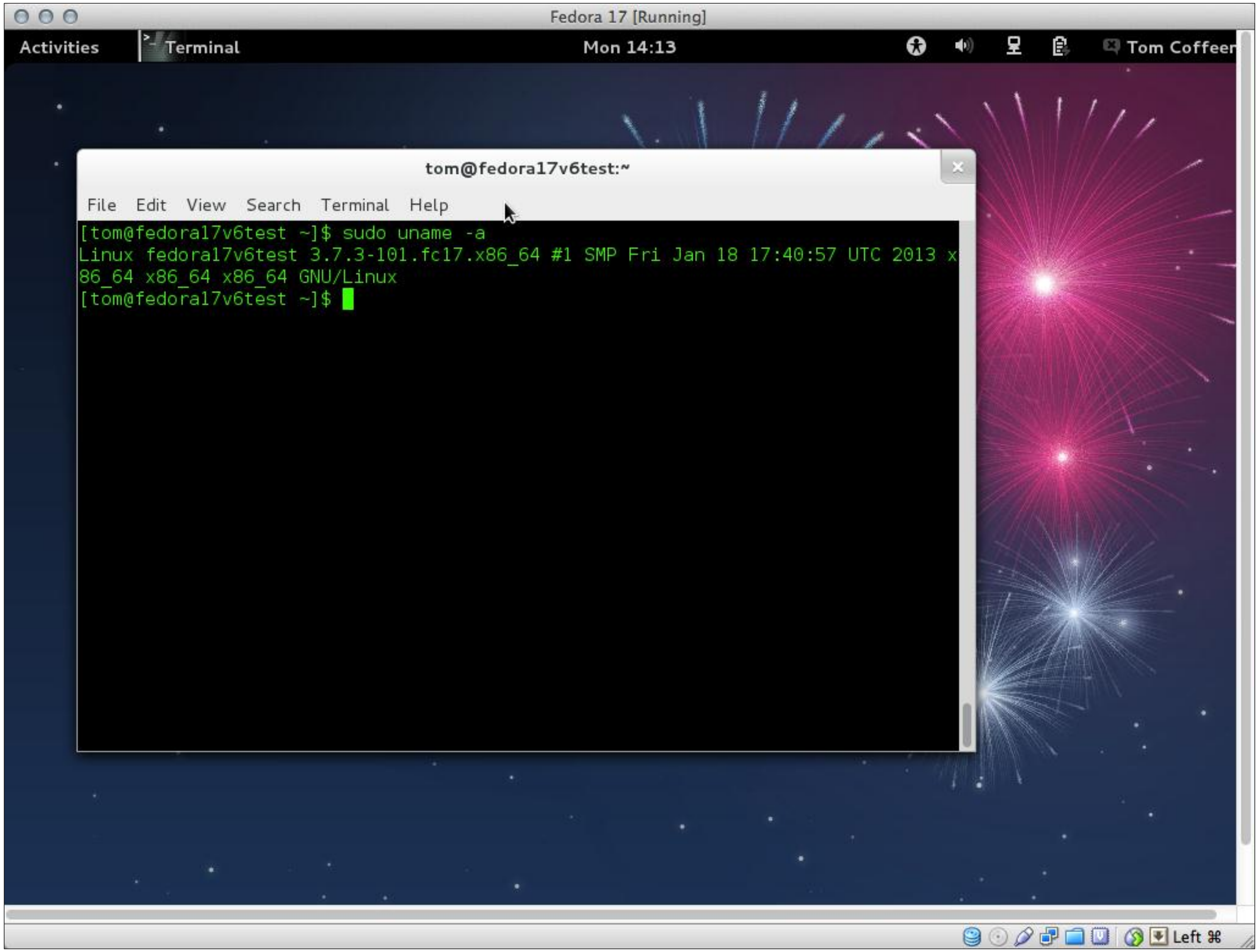
=

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

=

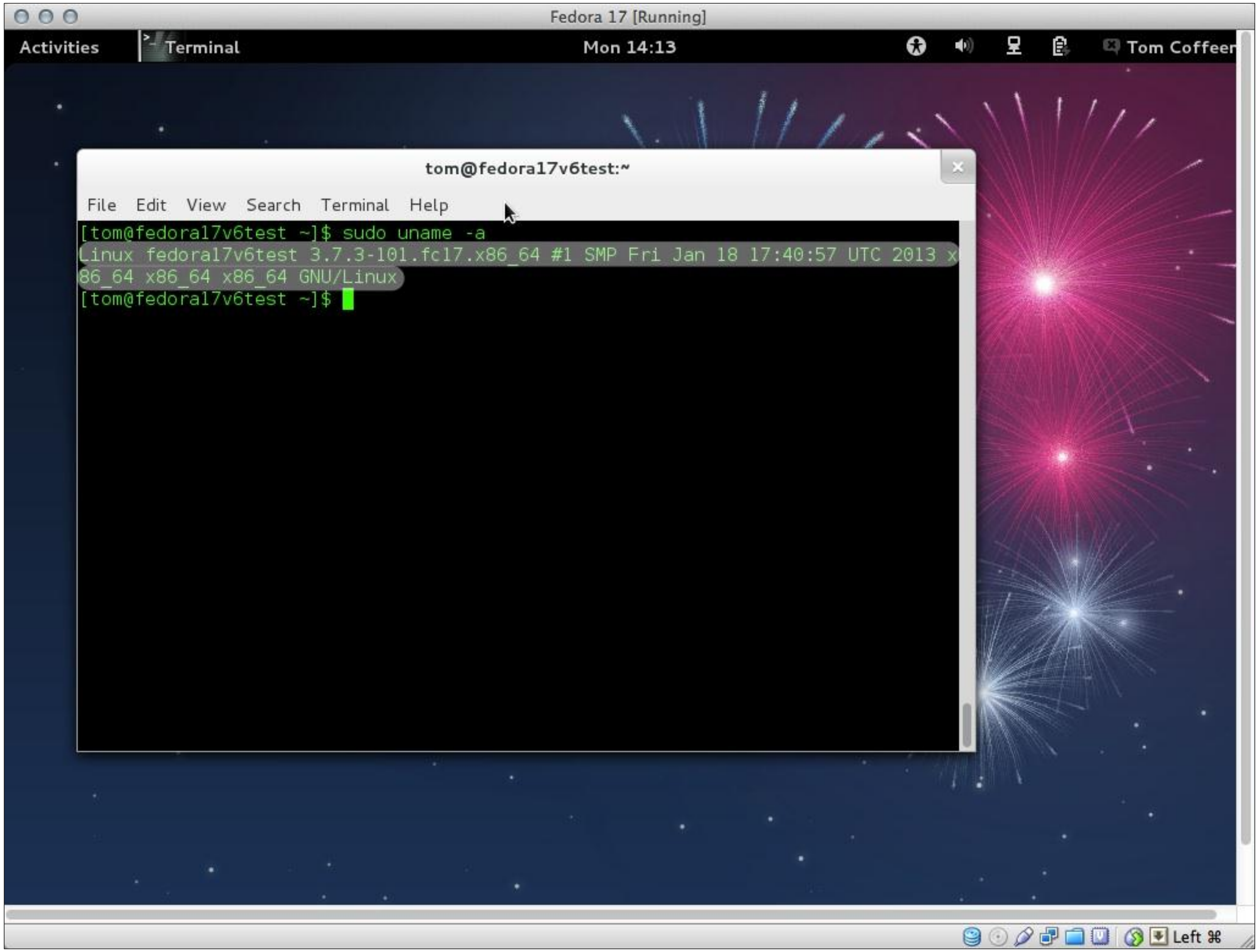
Fedora 17

DHCP Fingerprinting



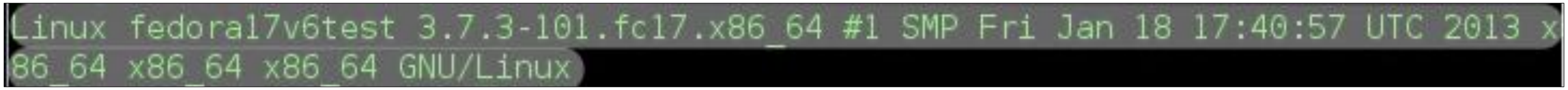
```
[tom@fedora17v6test ~]$ sudo uname -a
Linux fedora17v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x
86_64 x86_64 x86_64 GNU/Linux
[tom@fedora17v6test ~]$
```

DHCP Fingerprinting



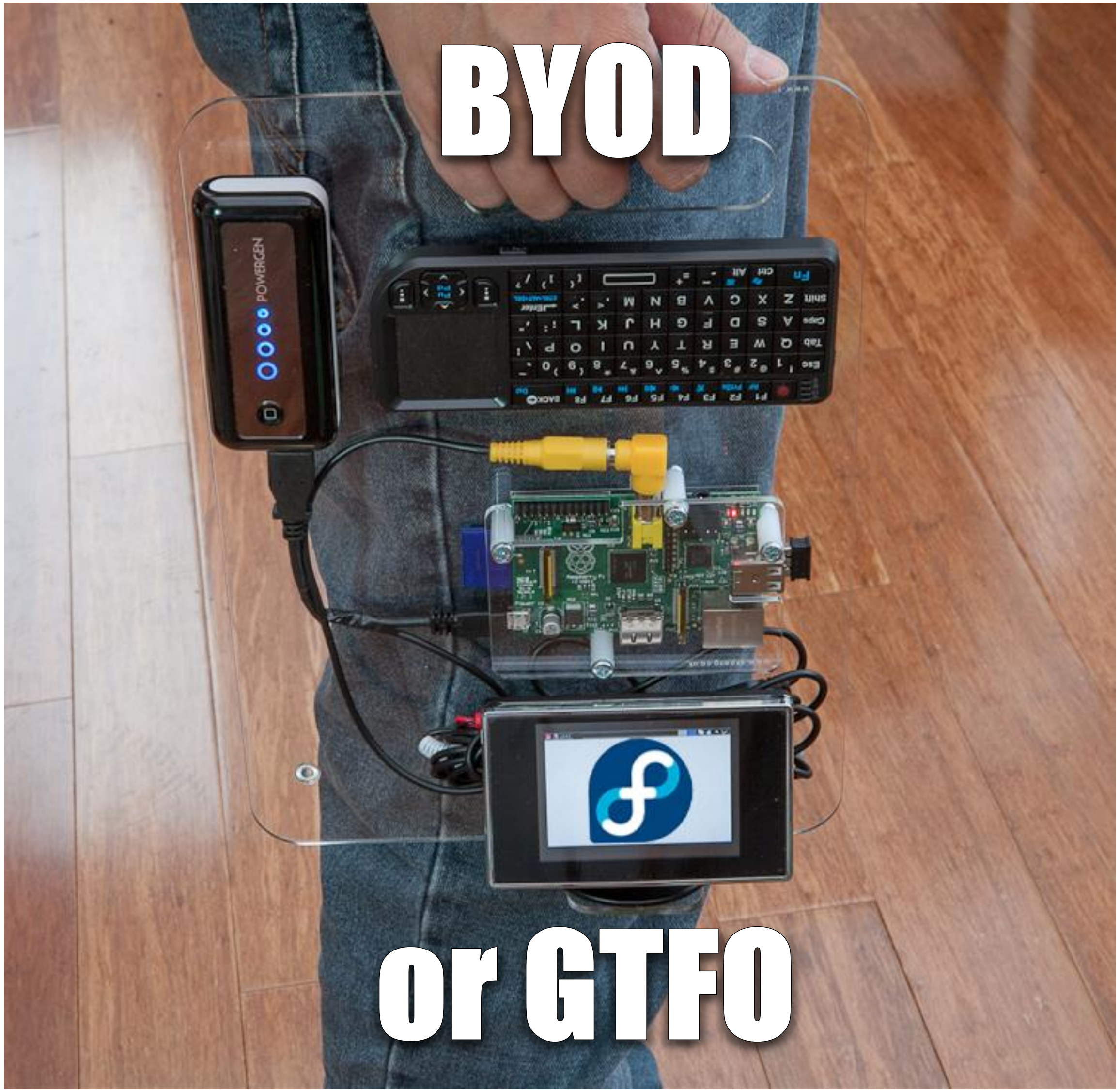
```
[tom@fedora17v6test ~]$ sudo uname -a
Linux fedora17v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x
86_64 x86_64 x86_64 GNU/Linux
[tom@fedora17v6test ~]$
```

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(v6) 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

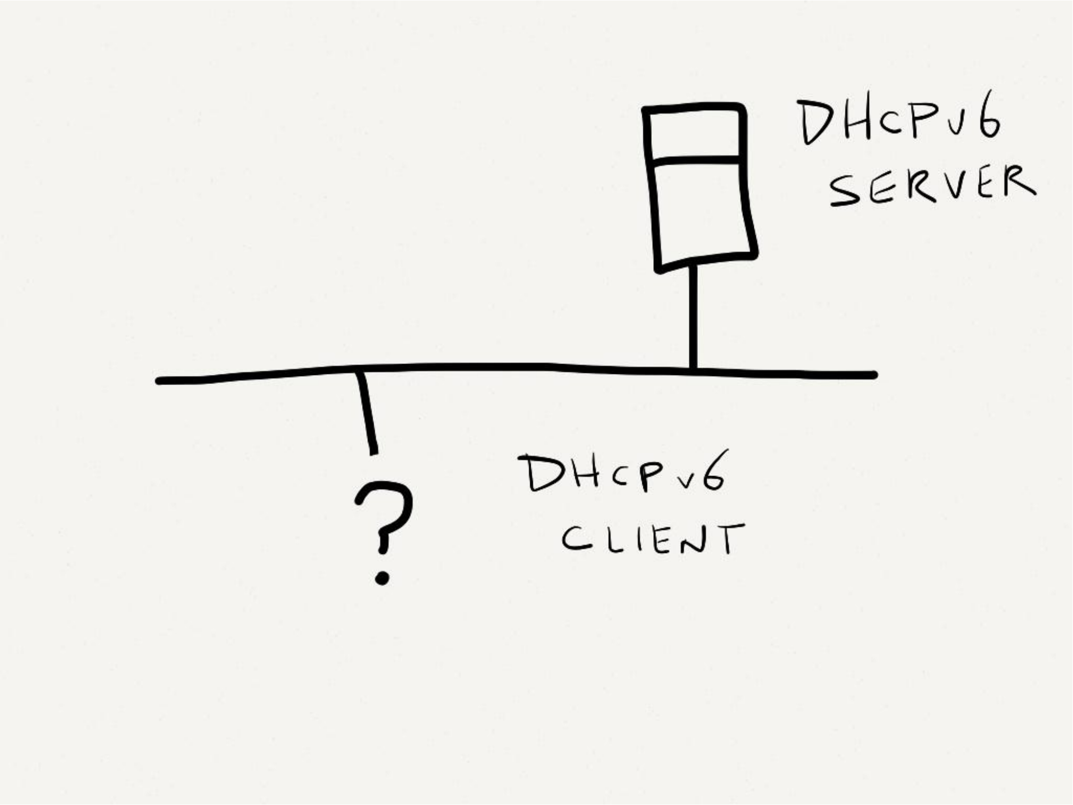
DHCP Fingerprinting

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-I605
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

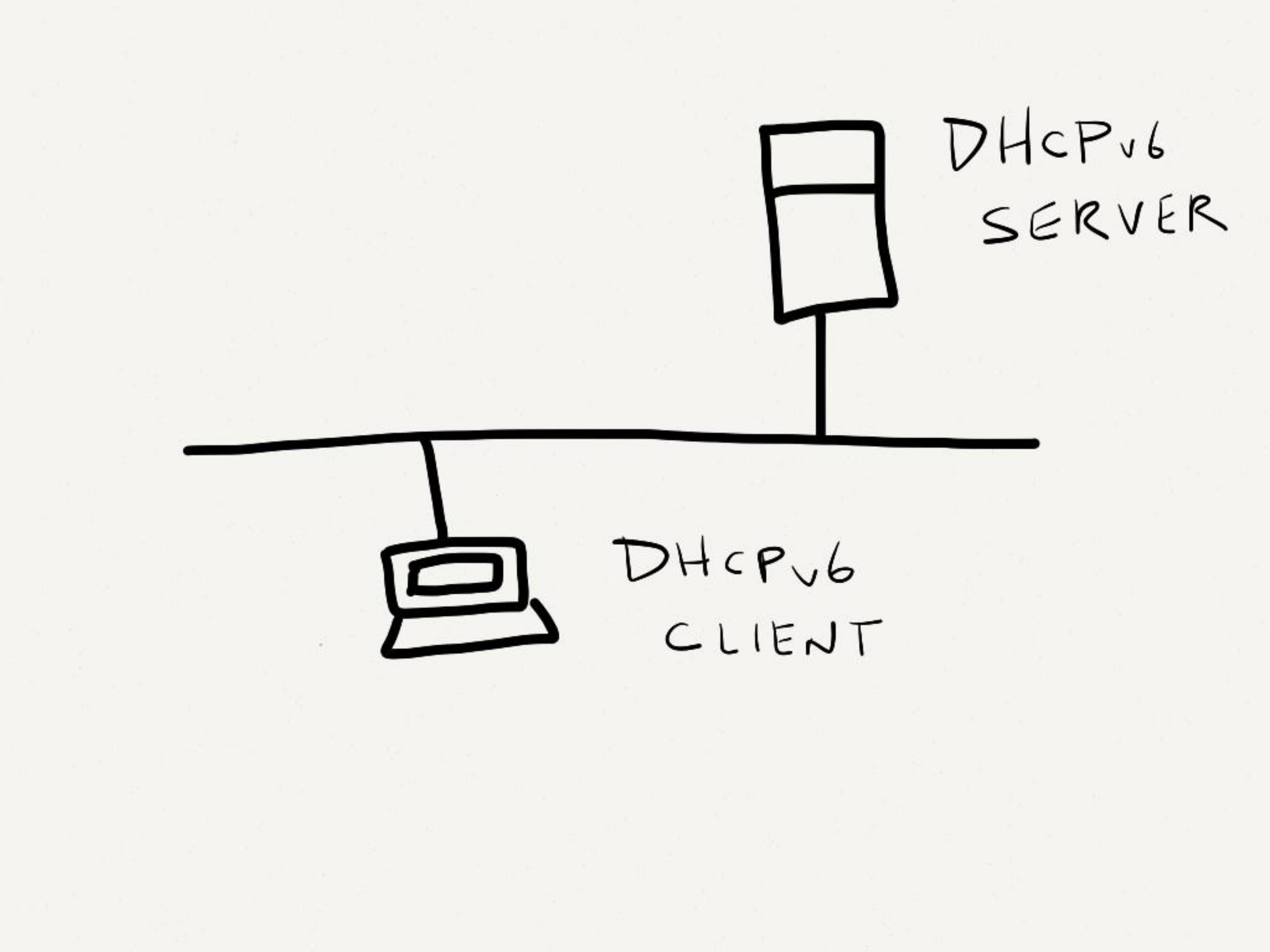
How is DHCPv6 fingerprinting different?

DHCPv6 Fingerprinting

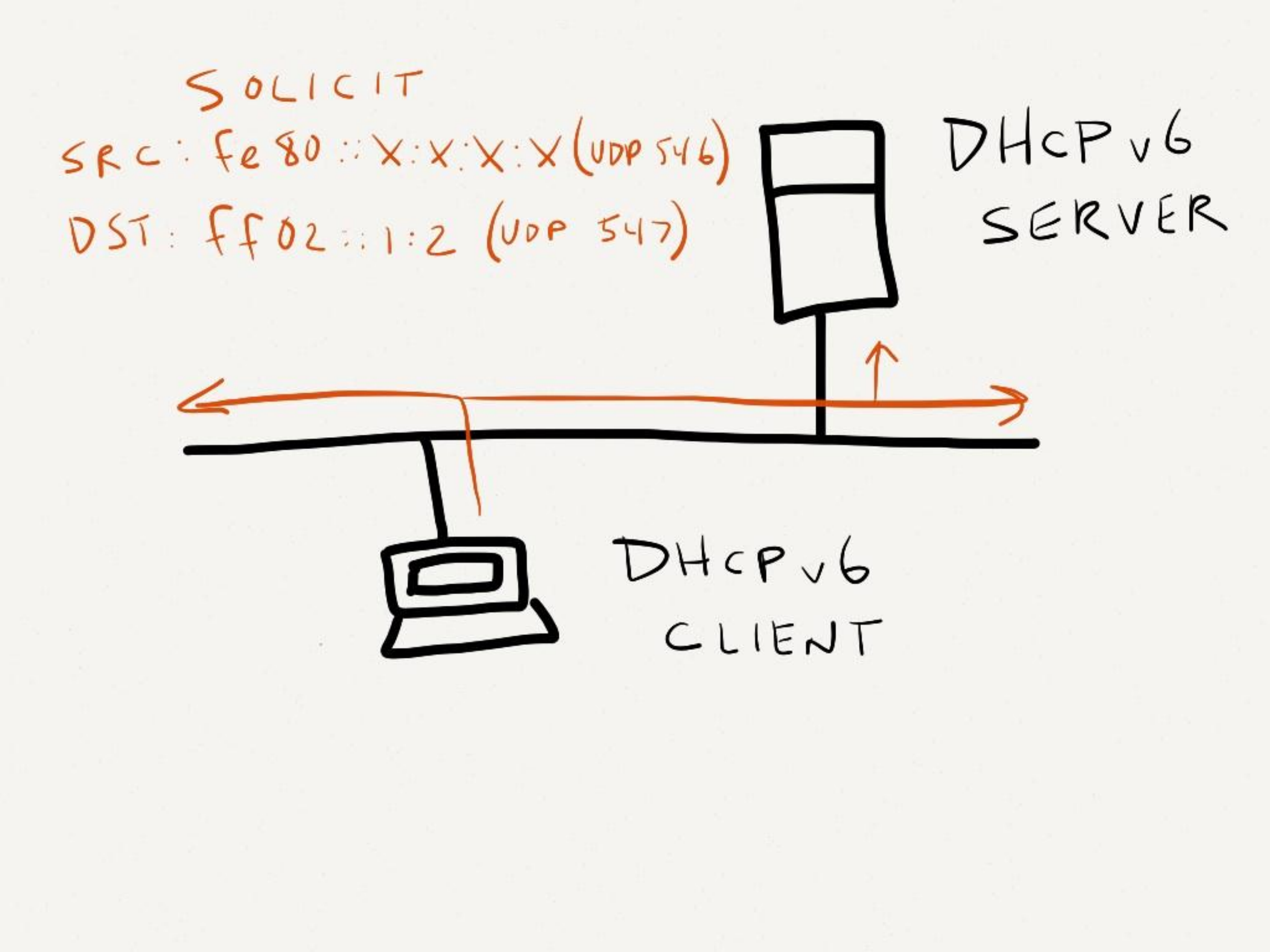


Same goal (client type), this time with DHCPv6

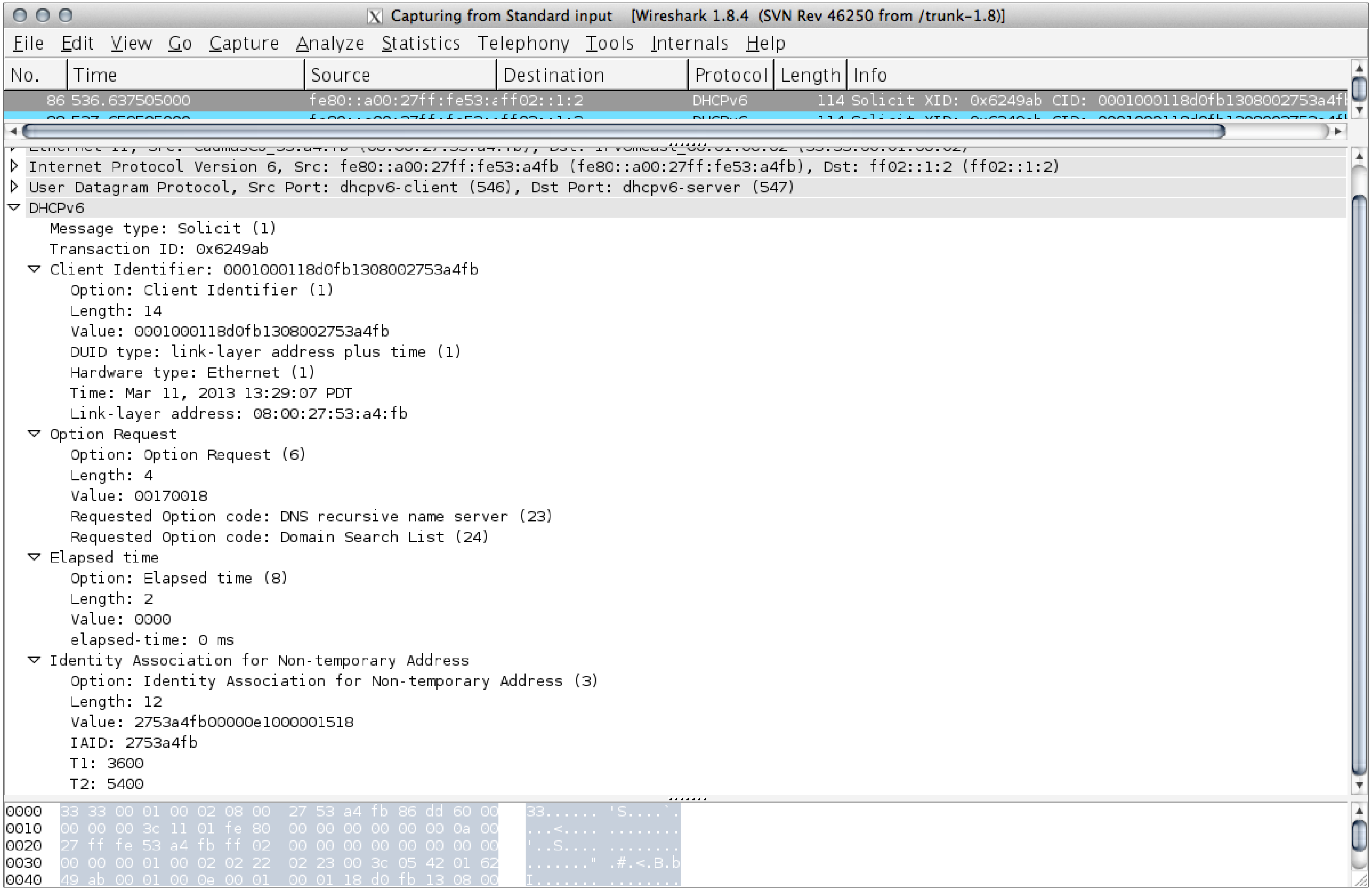
DHCPv6 Fingerprinting



DHCPv6 Fingerprinting



DHCPv6 Fingerprinting


Capturing from Standard input [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help

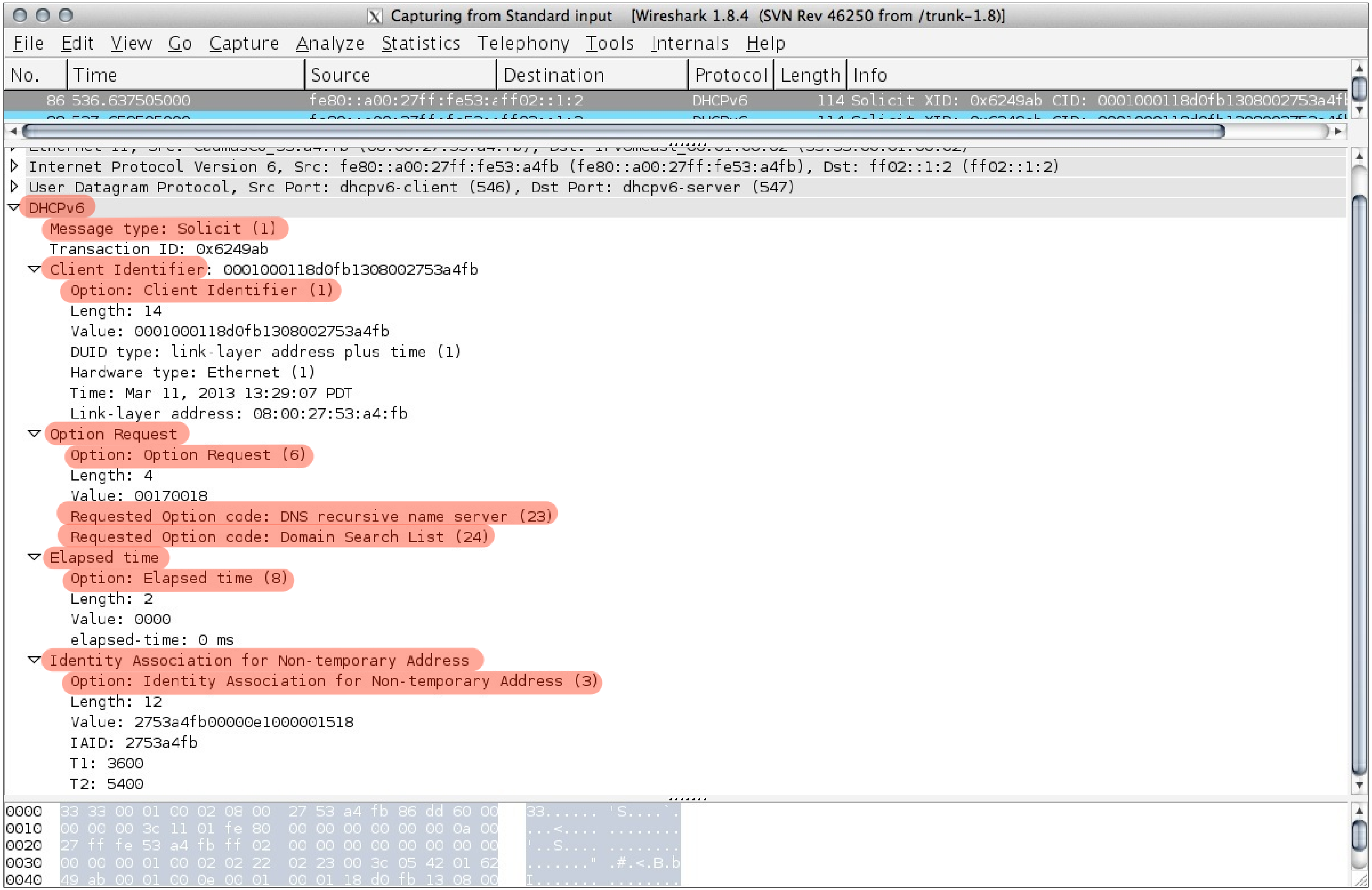
```
No.   Time            Source                  Destination   Protocol  Length  Info
   86 536.637505000   fe80::a00:27ff:fe53:a   ff02::1:2     DHCPv6       114  Solicit XID: 0x6249ab CID: 0001000118d0fb1308002753a4fb
```

```
▷ Internet Protocol Version 6, Src: fe80::a00:27ff:fe53:a4fb (fe80::a00:27ff:fe53:a4fb), Dst: ff02::1:2 (ff02::1:2)
▷ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
▽ DHCPv6
    Message type: Solicit (1)
    Transaction ID: 0x6249ab
  ▽ Client Identifier: 0001000118d0fb1308002753a4fb
      Option: Client Identifier (1)
      Length: 14
      Value: 0001000118d0fb1308002753a4fb
      DUID type: link-layer address plus time (1)
      Hardware type: Ethernet (1)
      Time: Mar 11, 2013 13:29:07 PDT
      Link-layer address: 08:00:27:53:a4:fb
  ▽ Option Request
      Option: Option Request (6)
      Length: 4
      Value: 00170018
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Domain Search List (24)
  ▽ Elapsed time
      Option: Elapsed time (8)
      Length: 2
      Value: 0000
      elapsed-time: 0 ms
  ▽ Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
      Length: 12
      Value: 2753a4fb00000e1000001518
      IAID: 2753a4fb
      T1: 3600
      T2: 5400
```

```
0000  33 33 00 01 00 02 08 00  27 53 a4 fb 86 dd 60 00   33...... 'S....`.
0010  00 00 00 3c 11 01 fe 80  00 00 00 00 00 00 0a 00   ...<.... ........
0020  27 ff fe 53 a4 fb ff 02  00 00 00 00 00 00 00 00   '..S.... ........
0030  00 00 00 01 00 02 02 22  02 23 00 3c 05 42 01 62   ......." .#.<.B.b
0040  49 ab 00 01 00 0e 00 01  00 01 18 d0 fb 13 08 00   I....... ........
```

Infoblox

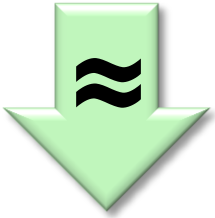
DHCPv6 Fingerprinting


Capturing from Standard input [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help

```
No.   Time               Source                  Destination      Protocol  Length  Info
   86 536.637505000      fe80::a00:27ff:fe53:a   ff02::1:2        DHCPv6       114  Solicit XID: 0x6249ab CID: 0001000118d0fb1308002753a4fb

▷ Ethernet II, Src: CadmusCo_53:a4:fb (08:00:27:53:a4:fb), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
▷ Internet Protocol Version 6, Src: fe80::a00:27ff:fe53:a4fb (fe80::a00:27ff:fe53:a4fb), Dst: ff02::1:2 (ff02::1:2)
▷ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
▽ DHCPv6
    Message type: Solicit (1)
    Transaction ID: 0x6249ab
  ▽ Client Identifier: 0001000118d0fb1308002753a4fb
      Option: Client Identifier (1)
      Length: 14
      Value: 0001000118d0fb1308002753a4fb
      DUID type: link-layer address plus time (1)
      Hardware type: Ethernet (1)
      Time: Mar 11, 2013 13:29:07 PDT
      Link-layer address: 08:00:27:53:a4:fb
  ▽ Option Request
      Option: Option Request (6)
      Length: 4
      Value: 00170018
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Domain Search List (24)
  ▽ Elapsed time
      Option: Elapsed time (8)
      Length: 2
      Value: 0000
      elapsed-time: 0 ms
  ▽ Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
      Length: 12
      Value: 2753a4fb00000e1000001518
      IAID: 2753a4fb
      T1: 3600
      T2: 5400

0000  33 33 00 01 00 02 08 00  27 53 a4 fb 86 dd 60 00   33...... 'S....`.
0010  00 00 00 3c 11 01 fe 80  00 00 00 00 00 00 0a 00   ...<.... ........
0020  27 ff fe 53 a4 fb ff 02  00 00 00 00 00 00 00 00   '..S.... ........
0030  00 00 00 01 00 02 02 22  02 23 00 3c 05 42 01 62   ......." .#.<.B.b
0040  49 ab 00 01 00 0e 00 01  00 01 18 d0 fb 13 08 00   I....... ........
```

DHCPv6 Fingerprinting

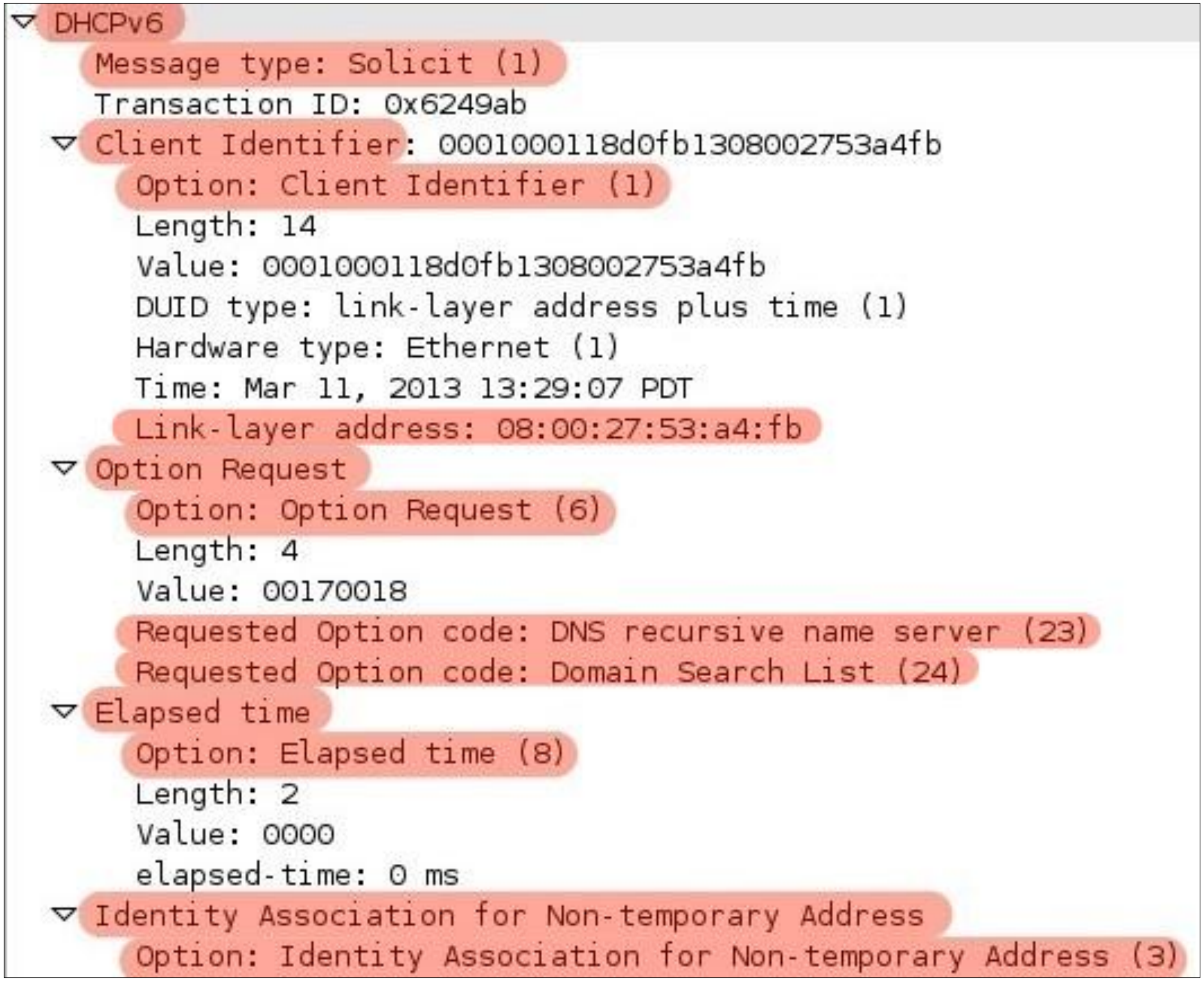
IPv4 DHCP Option Request (Option 55)



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
    Message type: Solicit (1)
    Transaction ID: 0x6249ab
  ▽ Client Identifier: 0001000118d0fb1308002753a4fb
      Option: Client Identifier (1)
      Length: 14
      Value: 0001000118d0fb1308002753a4fb
      DUID type: link-layer address plus time (1)
      Hardware type: Ethernet (1)
      Time: Mar 11, 2013 13:29:07 PDT
      Link-layer address: 08:00:27:53:a4:fb
  ▽ Option Request
      Option: Option Request (6)
      Length: 4
      Value: 00170018
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Domain Search List (24)
  ▽ Elapsed time
      Option: Elapsed time (8)
      Length: 2
      Value: 0000
      elapsed-time: 0 ms
  ▽ Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
```

Infoblox

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