Analysis of AS112 Traffic

Sid Faber
Network Situational Awareness Group
sfaber@cert.org

Problem Statement

What internal network topology data is exposed to the public Internet?

- Use security as a motivator for network administrators to block the traffic

Agenda

Overview of Data Sources

Data Analysis

- A queries
- PTR queries
- SOA queries
- UDP UPDATEs
- TCP UPDATEs
- TSIG names

Conclusions and Future Work

Data Sources:

DITL 2007 pcaps

Data Sources

- DITL 2007 AS112 packet captures
  - NaMeX (Italy)
    - 51 pcap files
    - Jan 8 @ 23:00 – Jan 11 @ 01:00
  - WIDE (Japan)
    - 50 pcap files
    - Jan 8 @ 23:45 – Jan 11 @ 00:00
  - *Are there any others available?*

Tools

- tcpdump
- dnsdump (Duane Wessels, John Kristoff)
  - Some customization to handle TCP & TSIG records
- Perl-fu, bash-fu

Data Analysis:

Queries

Data Analysis

General approach was to divide the traffic into a few bins, extract features, and run some trends

- A queries
- PTR queries
- SOA queries
- UDP UPDATEs
- TCP UPDATEs

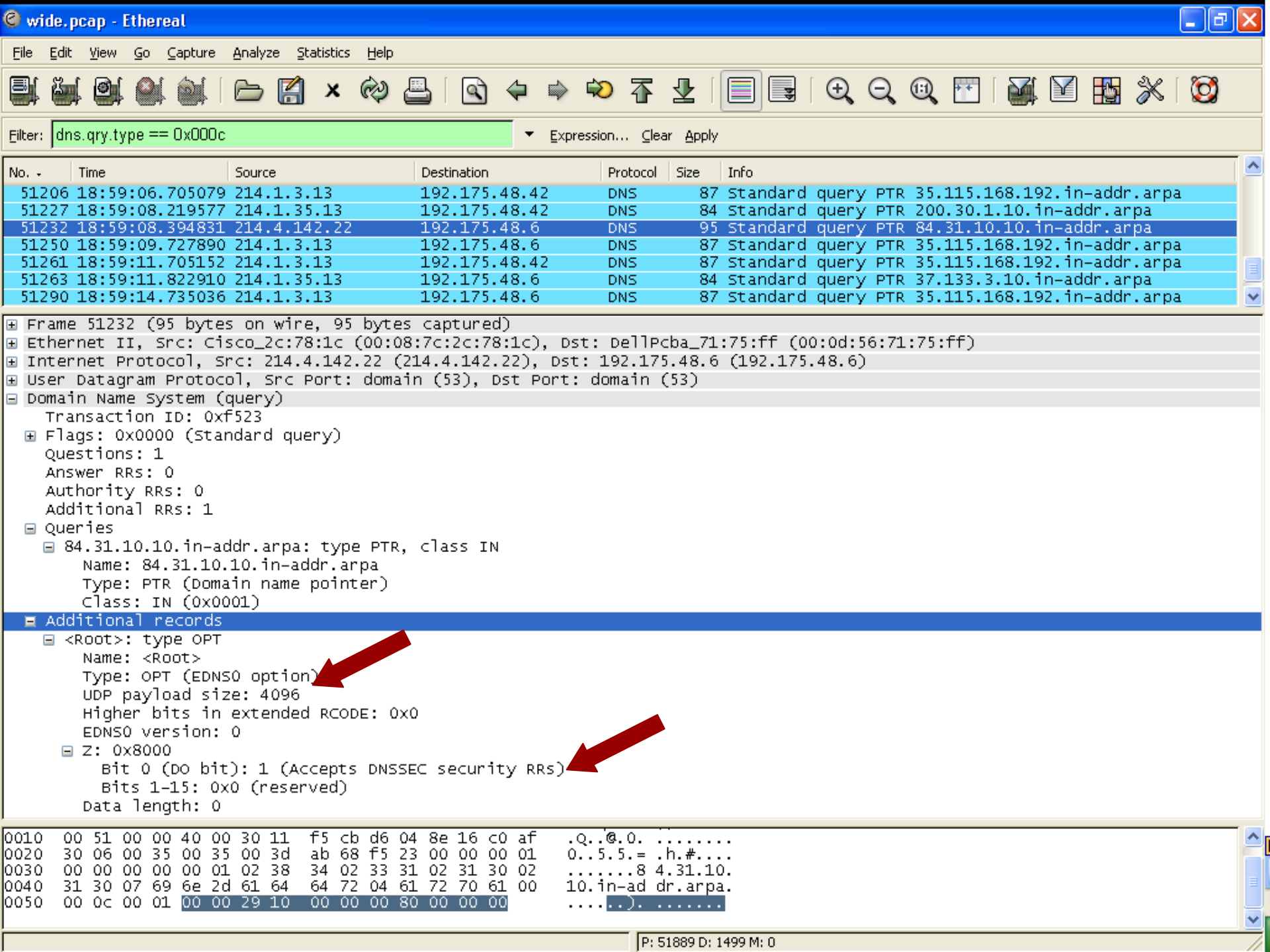
A queries

- Clients asking blackhole-1 and blackhole-2 for prisoner
- Results are not cached
  - Firewall blocking reply?
- Low volume, not very interesting
- No further trending

PTR queries

`dns.qry.type == 0x000c`

- Clients requesting the DNS name of an RFC1918 address
- Simple queries sent to blackhole-1 and blackhole-2
- Uniformity makes trending very easy
  - —Packets are mostly 81-88b
  - —Outliers are a little interesting


wide.pcap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: dns.qry.type == 0x000c
Expression... Clear Apply
No. Time Source Destination Protocol Size Info
51206 18:59:06.705079 214.1.3.13 192.175.48.42 DNS 87 Standard query PTR 35.115.168.192.in-addr.arpa
51227 18:59:08.219577 214.1.35.13 192.175.48.42 DNS 84 Standard query PTR 200.30.1.10.in-addr.arpa
51232 18:59:08.394831 214.4.142.22 192.175.48.6 DNS 95 Standard query PTR 84.31.10.10.in-addr.arpa
51250 18:59:09.727890 214.1.3.13 192.175.48.6 DNS 87 Standard query PTR 35.115.168.192.in-addr.arpa
51261 18:59:11.705152 214.1.3.13 192.175.48.42 DNS 87 Standard query PTR 35.115.168.192.in-addr.arpa
51263 18:59:11.822910 214.1.35.13 192.175.48.6 DNS 84 Standard query PTR 37.133.3.10.in-addr.arpa
51290 18:59:14.735036 214.1.3.13 192.175.48.6 DNS 87 Standard query PTR 35.115.168.192.in-addr.arpa
Frame 51232 (95 bytes on wire, 95 bytes captured)
Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:ff (00:0d:56:71:75:ff)
Internet Protocol, Src: 214.4.142.22 (214.4.142.22), Dst: 192.175.48.6 (192.175.48.6)
User Datagram Protocol, Src Port: domain (53), Dst Port: domain (53)
Domain Name System (query)
Transaction ID: 0xf523
Flags: 0x0000 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
84.31.10.10.in-addr.arpa: type PTR, class IN
Name: 84.31.10.10.in-addr.arpa
Type: PTR (Domain name pointer)
Class: IN (0x0001)
Additional records
<Root>: type OPT
Name: <Root>
Type: OPT (EDNS0 option)
UDP payload size: 4096
Higher bits in extended RCODE: 0x0
EDNS0 version: 0
Z: 0x8000
Bit 0 (DO bit): 1 (Accepts DNSSEC security RRs)
Bits 1-15: 0x0 (reserved)
Data length: 0
0010 00 51 00 00 40 00 30 11 f5 cb d6 04 8e 16 c0 af .Q..@.0. ....
0020 30 06 00 35 00 35 00 3d ab 68 f5 23 00 00 00 01 0..5.5.= .h.#....
0030 00 00 00 00 00 01 02 38 34 02 33 31 02 31 30 02 ....8 4.31.10.
0040 31 30 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 10.in-ad dr.arpa.
0050 00 0c 00 01 00 00 29 10 00 00 00 80 00 00 00 00 ....). ....
P: 51889 D: 1499 M: 0

PTR queries

`dns.qry.type == 0x000c`

- Clients requesting the DNS name of an RFC1918 address
- Simple queries sent to blackhole-1 and blackhole-2
- Uniformity makes trending very easy
  - Packets are mostly 81-88b
  - Outliers are a little interesting
- Not much of interest, no further trending

SOA queries

```
(dns.qry.type==0x0006)&&
(dns.flags.opcode==0)
```

- Sent to blackhole-1 and blackhole-2
- Clients looking for somewhere to send UPDATEs.
- Some request the entire address
  - SOA 120.130.1.10.in-addr.arpa
  - Recursion not desired
- Some request the block
  - 10.in-addr.arpa
  - Recursion desired
- Some have an EDNS0 record

SOA queries (2)

SOA Conclusions

- Might be useful to map out some internal addresses
- Might help fingerprint
- Further studies might help understand more fully
- No surprises, still not much of interest

Data Analysis:

UDP UPDATEs

UDP UPDATEs

```
(ip.proto==0x11)&&(dns.flags.opcode==5)
```

- Packets destined to prisoner (as expected)
- Two general formats

UDP UPDATEs Form 1: Short

No.	Time	Source	Destination	Size	Protocol	Info
448	2007-01-10 18:02:24.484252	214.13.190.178	192.175.48.1	126	DNS	Dynamic update SOA 10.in-ad
261	2007-01-10 18:01:15.404592	214.13.190.178	192.175.48.1	127	DNS	Dynamic update SOA 10.in-ad
8450	2007-01-10 18:43:20.498391	214.13.190.178	192.175.48.1	128	DNS	Dynamic update SOA 10.in-ad
9161	2007-01-10 18:47:45.635241	214.13.190.178	192.175.48.1	128	DNS	Dynamic update SOA 10.in-ad
11258	2007-01-10 18:58:58.914932	214.13.190.178	192.175.48.1	128	DNS	Dynamic update SOA 10.in-ad

```
⊞ Frame 9161 (128 bytes on wire, 128 bytes captured)
⊞ Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
⊞ Internet Protocol, Src: 214.13.190.178 (214.13.190.178), Dst: 192.175.48.1 (192.175.48.1)
⊞ User Datagram Protocol, Src Port: 6615 (6615), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x0762
  ⊞ Flags: 0x2800 (Dynamic update)
    Zones: 1
    Prerequisites: 0
    Updates: 1
    Additional RRs: 0
  ⊟ Zone
    ⊟ 10.in-addr.arpa: type SOA, class IN
        Name: 10.in-addr.arpa
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
  ⊟ Updates
    ⊟ 131.100.87.10.in-addr.arpa: type PTR, class IN, stevecomputer
        Name: 131.100.87.10.in-addr.arpa
        Type: PTR (Domain name pointer)
        Class: IN (0x0001)
        Time to live: 15 minutes
        Data length: 15
        Domain name: stevecomputer
```

One zone SOA record in the Query slot

One PTR UPDATE record , class IN, in the NS/Auth slot

```
0000  00 0d 56 71 75 f7 00 08  7c 2c 78 1c 08 00 45 00   ..Vqu... |,x...E.
0010  00 72 be b9 00 00 6c 11  0a 51 d6 0d be b2 c0 af   .r....l. .Q......
0020  30 01 19 d7 00 35 00 5e  a6 7d 07 62 28 00 00 01   0....5.^ .}.b(...
0030  00 00 00 01 00 00 02 31  30 07 69 6e 2d 61 64 64   .......1 0.in-add
0040  72 04 61 72 70 61 00 00  06 00 01 03 31 33 31 03   r.arpa.. ....131.
0050  31 30 30 02 38 37 02 31  30 07 69 6e 2d 61 64 64   100.87.1 0.in-add
0060  72 04 61 72 70 61 00 00  0c 00 01 00 00 03 84 00   r.arpa.. ........
0070  0f 0d 73 74 65 76 65 63  6f 6d 70 75 74 65 72 00   ..stevec omputer.
```

File: "C:/Documents and Settings/sfaber/Desktop/step3.pcap" 2031 KB 00:59:59

P: 11440 D: 10808 M: 0

UDP UPDATEs Form 1: Key Features

No.	Time	Source	Destination	Size	Protocol	Info
448	2007-01-10 18:02:24.484252	214.13.190.178	192.175.48.1	126	DNS	Dynamic update SOA 10.in-ad
261	2007-01-10 18:01:15.404592	214.13.190.178	192.175.48.1	127	DNS	Dynamic update SOA 10.in-ad
8450	2007-01-10 18:43:20.498391	214.13.190.178	192.175.48.1	128	DNS	Dynamic update SOA 10.in-ad
9161	2007-01-10 18:47:45.635241	214.13.190.178	192.175.48.1	128	DNS	Dynamic update SOA 10.in-ad
11258	2007-01-10 18:58:58.914932	214.13.190.178	192.175.48.1	128	DNS	Dynamic update SOA 10.in-ad

```
Frame 9161 (128 bytes on wire, 128 bytes captured)
Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
Internet Protocol, Src: 214.13.190.178 (214.13.190.178), Dst: 192.175.48.1 (192.175.48.1)
User Datagram Protocol, Src Port: 6615 (6615), Dst Port: domain (53)
Domain Name System (query)
    Transaction ID: 0x0762
  Flags: 0x2800 (Dynamic update)
    Zones: 1
    Prerequisites: 0
    Updates: 1
    Additional RRs: 0
  Zone
    10.in-addr.arpa: type SOA, class IN
        Name: 10.in-addr.arpa
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
  Updates
    131.100.87.10.in-addr.arpa: type PTR, class IN, stevecomputer
        Name: 131.100.87.10.in-addr.arpa
        Type: PTR (Domain name pointer)
        Class: IN (0x0001)
        Time to live: 15 minutes
        Data length: 15
        Domain name: stevecomputer
```

Gateway Address

Private Address

Private Name

```
0000  00 0d 56 71 75 f7 00 08  7c 2c 78 1c 08 00 45 00   ..Vqu... |,x...E.
0010  00 72 be b9 00 00 6c 11  0a 51 d6 0d be b2 c0 af   .r....l. .Q......
0020  30 01 19 d7 00 35 00 5e  a6 7d 07 62 28 00 00 01   0....5.^ .}.b(...
0030  00 00 00 01 00 00 02 31  30 07 69 6e 2d 61 64 64   .......1 0.in-add
0040  72 04 61 72 70 61 00 00  06 00 01 03 31 33 31 03   r.arpa.. ....131.
0050  31 30 30 02 38 37 02 31  30 07 69 6e 2d 61 64 64   100.87.1 0.in-add
0060  72 04 61 72 70 61 00 00  0c 00 01 00 00 03 84 00   r.arpa.. ........
0070  0f 0d 73 74 65 76 65 63  6f 6d 70 75 74 65 72 00   ..stevec omputer.
```

File: "C:/Documents and Settings/sfaber/Desktop/step3.pcap" 2031 KB 00:59:59

P: 11440 D: 10808 M: 0

UDP UPDATEs Form 2: Long

No.	Time	Source	Destination	Size	Protocol	Info
9860	2007-01-10 18:51:49.901117	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa
9878	2007-01-10 18:51:53.520995	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa
10689	2007-01-10 18:56:01.658796	214.1.24.169	192.175.48.1	157	DNS	Dynamic update SOA 168.192.in-addr.
10863	2007-01-10 18:56:58.962171	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa
10873	2007-01-10 18:57:01.134500	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa

```
⊞ Internet Protocol, Src: 214.13.190.178 (214.13.190.178), Dst: 192.175.48.1 (192.175.48.1)
⊞ User Datagram Protocol, Src Port: 6803 (6803), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x9350
  ⊞ Flags: 0x2800 (Dynamic update)
    Zones: 1
    Prerequisites: 1
    Updates: 2
    Additional RRs: 0
  ⊟ Zone
    ⊞ 10.in-addr.arpa: type SOA, class IN
  ⊟ Prerequisites
    ⊟ 6.0.0.10.in-addr.arpa: type CNAME, class NONE
        Name: 6.0.0.10.in-addr.arpa
        Type: CNAME (Canonical name for an alias)
        Class: NONE (0x00fe)
        Time to live: 0 time
        Data length: 0
  ⊟ Updates
    ⊟ 6.0.0.10.in-addr.arpa: type PTR, class ANY
        Name: 6.0.0.10.in-addr.arpa
        Type: PTR (Domain name pointer)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 0
    ⊟ 6.0.0.10.in-addr.arpa: type PTR, class IN, mc4-36-006.MC4MED.local
        Name: 6.0.0.10.in-addr.arpa
        Type: PTR (Domain name pointer)
        Class: IN (0x0001)
        Time to live: 20 minutes
        Data length: 25
        Domain name: mc4-36-006.MC4MED.local
```

One zone SOA record in the Query slot

A CNAME prereq in the ANS slot

First PTR update, class ANY in the NS/Auth slot

Second PTR update, class IN

```
0060  61 00 00 05 00 fe 00 00  00 00 00 00 c0 21 00 0c   a....... .....!..
0070  00 ff 00 00 00 00 00 00  c0 21 00 0c 00 01 00 00   ........ .!......
0080  04 b0 00 19 0a 6d 63 34  2d 33 36 2d 30 30 36 06   .....mc4 -36-006.
0090  4d 43 34 4d 45 44 05 6c  6f 63 61 6c 00            MC4MED.l ocal.
```

P: 11440 D: 10808 M: 0

UDP UPDATEs Form 2: Key Features

No.	Time	Source	Destination	Size	Protocol	Info
9860	2007-01-10 18:51:49.901117	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa
9878	2007-01-10 18:51:53.520995	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa
10689	2007-01-10 18:56:01.658796	214.1.24.169	192.175.48.1	157	DNS	Dynamic update SOA 168.192.in-addr.
10863	2007-01-10 18:56:58.962171	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa
10873	2007-01-10 18:57:01.134500	214.13.190.178	192.175.48.1	157	DNS	Dynamic update SOA 10.in-addr.arpa

```
⊞ Internet Protocol, Src: 214.13.190.178 (214.13.190.178), Dst: 192.175.48.1 (192.175.48.1)
⊞ User Datagram Protocol, Src Port: 6803 (6803), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x9350
  ⊞ Flags: 0x2800 (Dynamic update)
    Zones: 1
    Prerequisites: 1
    Updates: 2
    Additional RRs: 0
  ⊟ Zone
    ⊞ 10.in-addr.arpa: type SOA, class IN
  ⊟ Prerequisites
    ⊟ 6.0.0.10.in-addr.arpa: type CNAME, class NONE
        Name: 6.0.0.10.in-addr.arpa
        Type: CNAME (Canonical name for an alias)
        Class: NONE (0x00fe)
        Time to live: 0 time
        Data length: 0
  ⊟ Updates
    ⊟ 6.0.0.10.in-addr.arpa: type PTR, class ANY
        Name: 6.0.0.10.in-addr.arpa
        Type: PTR (Domain name pointer)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 0
    ⊟ 6.0.0.10.in-addr.arpa: type PTR, class IN, mc4-36-006.MC4MED.local
        Name: 6.0.0.10.in-addr.arpa
        Type: PTR (Domain name pointer)
        Class: IN (0x0001)
        Time to live: 20 minutes
        Data length: 25
        Domain name: mc4-36-006.MC4MED.local
```

```
0060  61 00 00 05 00 fe 00 00  00 00 00 00 c0 21 00 0c   a....... .....!..
0070  00 ff 00 00 00 00 00 00  c0 21 00 0c 00 01 00 00   ........ .!......
0080  04 b0 00 19 0a 6d 63 34  2d 33 36 2d 30 30 36 06   .....mc4 -36-006.
0090  4d 43 34 4d 45 44 05 6c  6f 63 61 6c 00            MC4MED.l ocal.
```

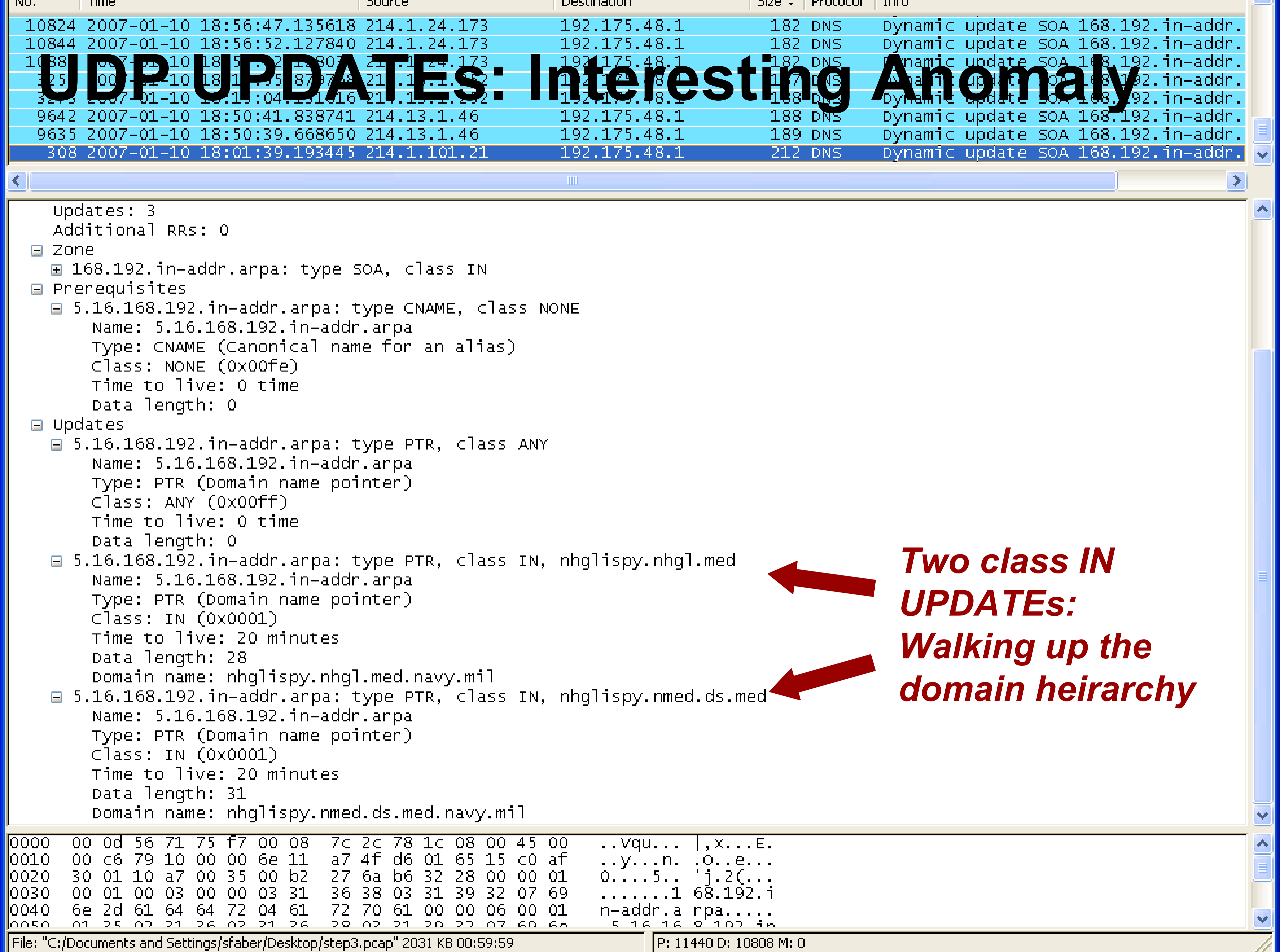
P: 11440 D: 10808 M: 0

Gateway Address

Private Address

Private Name (and sometimes domain)

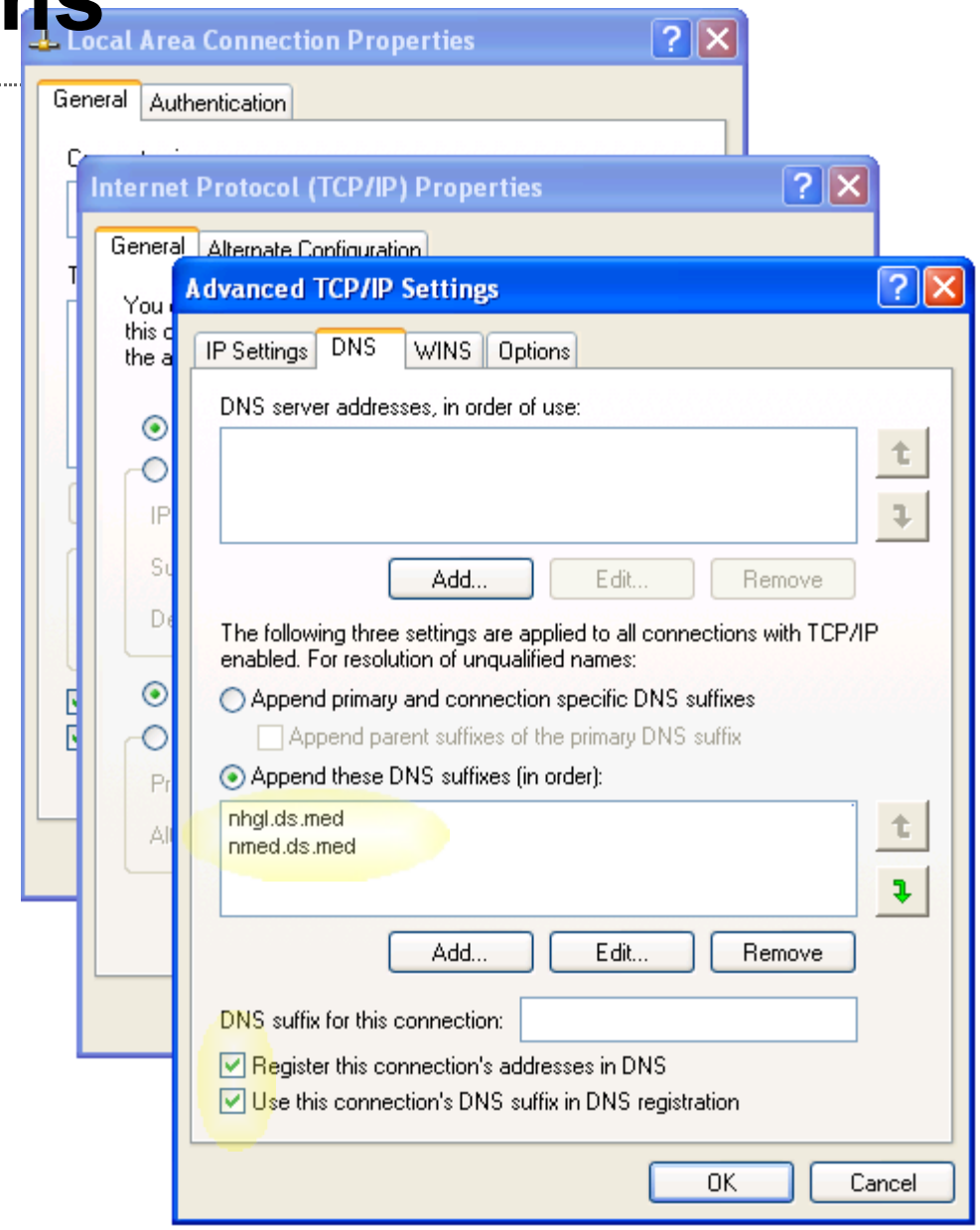
UDP UPDATEs: Interesting Anomaly



Two class IN UPDATEs: Walking up the domain heirarchy

UDP UPDATE Forms

- Might relate to assigned DNS suffixes?



UDP UPDATEs: Stats

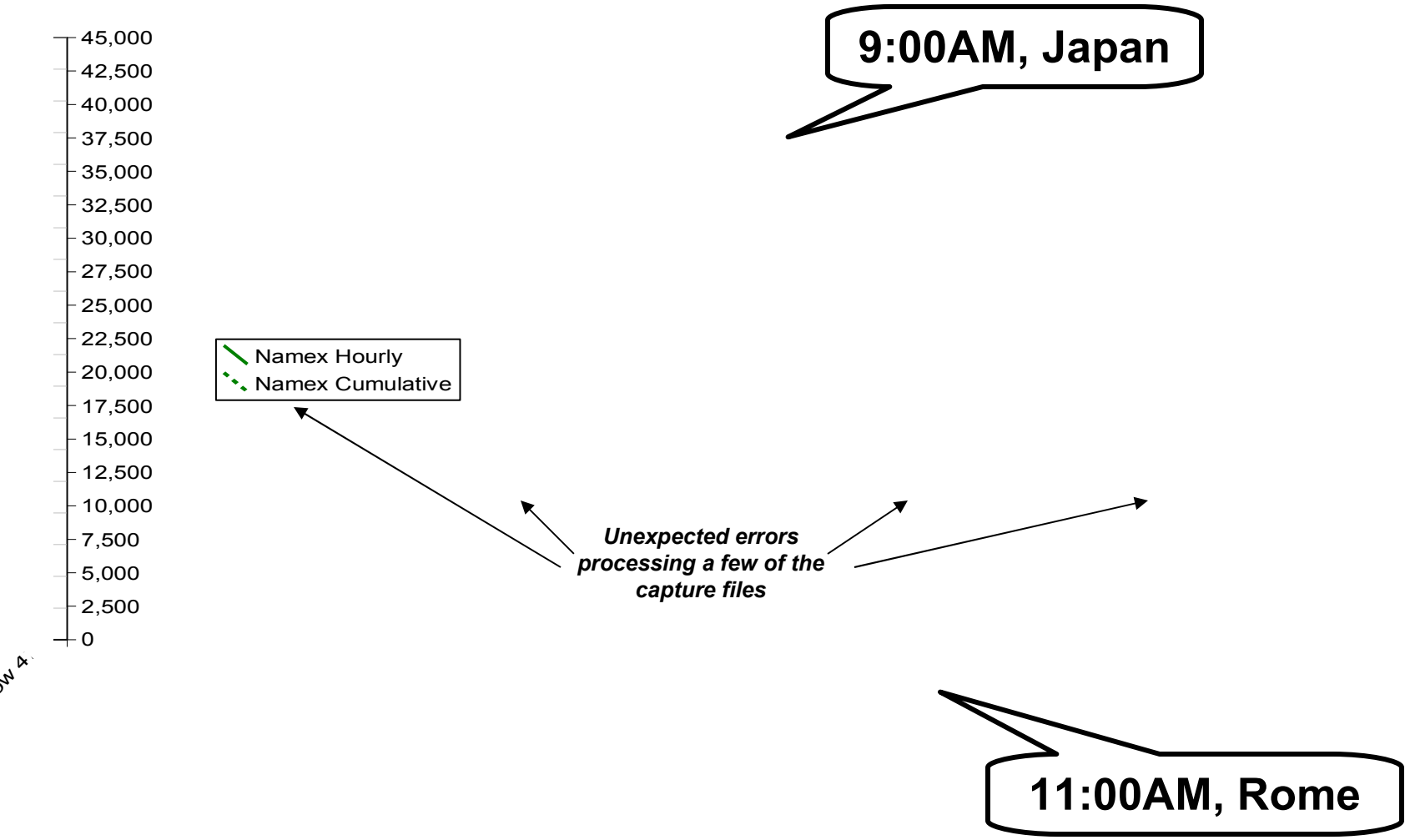
Unique Entries		
NaMeX	402,135	(18.7%)
WIDE	1,743,505	(81.3%)
Total	2,145,226	
Overlap	414*	(0.02%)
No Domain	401,977	(18.7%)
Gateways	616,618	

*Overlap:

204.10.216.0/21 (Education Co-op in Cincinatti) had 2000+ total clients; 18% (353) hit both NaMeX and WIDE through one of 11 gateways.

Also 70.63.30.170 (Roadrunner) hit both NaMeX and WIDE with various hosts

UDP UPDATEs: Arrival Rate



UDP UPDATEs: Most Popular Gateways

Clients	Gateway	Owner
26,285	65.120.80.8	Qwest Communications
15,947	65.117.145.11	Qwest Communications
15,090	202.21.158.18	Republic Polytechnic, Singapore
8,796	210.53.201.160	CNCGroup IP network, China
6,483	206.80.195.18	Qwest Communications
6,295	204.228.117.202	WestNet, Inc, Boulder, CO
5,831	202.39.57.251	Chunghwa Telecom Co., Ltd., Taiwan
5,170	202.42.255.254	Singapore General Hospital, Singapore
4,815	203.127.180.234	SingNet Pte Ltd, Singapore
4,202	66.77.163.198	Qwest Communications

UDP UPDATEs: Most Popular Private /24's

Clients	Private /24
255,322	192.168.1.0/24
174,708	192.168.0.0/24
48,096	192.168.2.0/24
39,811	10.0.0.0/24
36,300	192.168.10.0/24
27,710	192.168.100.0/24
22,651	192.168.3.0/24
17,192	192.168.11.0/24
15,154	192.168.5.0/24
13,299	10.1.1.0/24

11.9%

8.1%

Clients	Private /24
12,484	192.168.20.0/24
12,334	192.168.4.0/24
12,009	172.16.1.0/24
9,933	10.5.0.0/24
9,588	10.10.10.0/24
9,166	192.168.6.0/24
9,058	172.16.2.0/24
8,944	192.168.8.0/24
8,642	10.0.1.0/24
8,421	10.14.36.0/24

*Rankings are nearly identical whether counting ***gateways*** or ***clients*** using a /24

UDP UPDATEs: Most Popular Client Names

Count	Name
12,187	server
2,430	admin
1,691	server1
1,593	server01
937	pc01
836	pc02
802	reception
802	pc03
785	toshiba-user
785	computer

0.5%

Count	Name
764	pc04
708	user
705	frontdesk
687	laptop
642	pc05
605	pc06
593	server2
577	pc11
563	mail
553	server2003

Why so many servers? Are these DHCP servers? DNS Servers? Gateways?

UDP UPDATEs: Most Popular TLD

Count	Name
434,106	local
401,979	[no TLD]
376,808	com
137,814	tw
112,570	us
97,057	jp
82,894	edu
82,009	org
76,556	net
46,028	sg

20.2%

18.7%

Count	Name
24,299	my
21,832	lcl
15,750	it
13,119	corp
10,761	kr
7,111	cn
6,839	loc
6,206	locale
6,043	int
5,558	intra

Data Analysis:

TCP UPDATEs

TCP UPDATEs

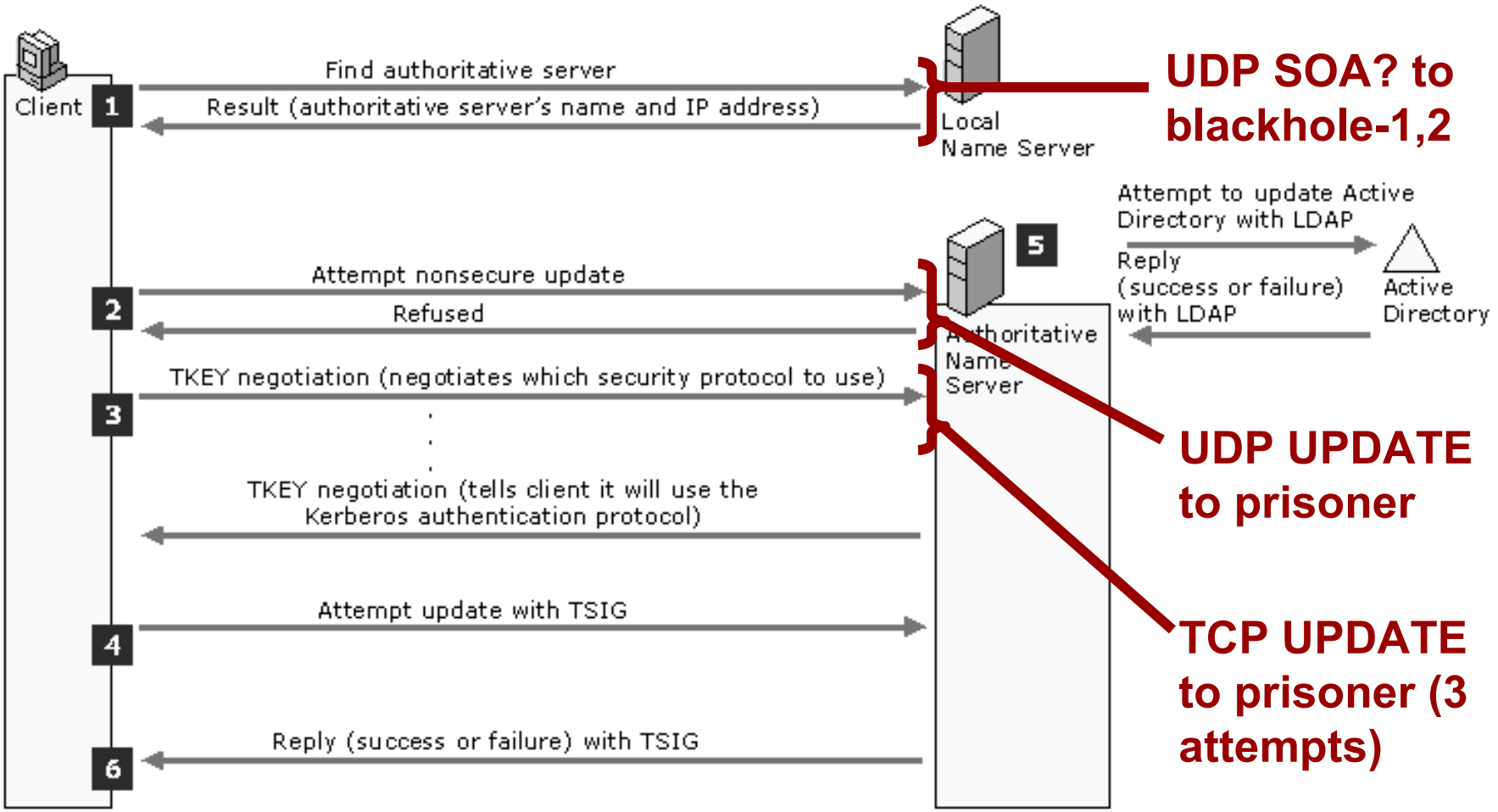
```
(ip.proto==0x06)
```

- Packets destined to prisoner
- Well-formed TCP connection
  - —SYN, SYN-ACK, ACK
  - —One packet of data
  - —FIN, ACK, FIN, ACK

TCP UPDATEs (2)

- Part of a larger conversation
  - UDP UPDATE request
  - Three TCP UPDATE attempts
- Does the TCP UPDATE have additional information?
  - Yes, it's actually sending a TKEY record
  - Again, there are two general formats

TCP UPDATEs the Microsoft Way



Source: Windows 2000 Server Resource Kit, DNS / Dynamic and Secure Dynamic Update, www.microsoft.com

Microsoft Implementation Notes

From KB article 816592:

- Clients that are running Windows Server 2003, Windows 2000, or Windows XP DHCP interact with DNS dynamic update protocol in the following manner:
  - The client initiates a DHCP request message (DHCPREQUEST) to the server. The request includes option 81.
  - The server returns a DHCP acknowledgement message (DHCPACK) to the client. The client grants an IP address lease and includes option 81. If the DHCP server is configured with the default settings, option 81 tells the client that the DHCP server will register the DNS PTR record and that the client will register the DNS A record.
  - Asynchronously, the ***client*** sends a DNS update request to the DNS server for its own forward lookup record, a host A resource record.
  - The ***DHCP server*** registers the PTR record of the client.
- By default, Windows XP and Windows Server 2003 reregister their A and PTR resource records every 24 hours regardless of the computer's role.

TCP TKEY Form 1: Windows 2000

```
    8 2007-01-10 18:01:40.614815 214.1.101.21   192.175.48.1    62 TCP    4271 > domain [SYN] Seq=0 Ack=0 Win=16384
   10 2007-01-10 18:01:40.876805 214.1.101.21   192.175.48.1    60 TCP    4271 > domain [ACK] Seq=1 Ack=0 Win=16560
   11 2007-01-10 18:01:40.877095 214.1.101.21   192.175.48.1   203 DNS    Standard query TKEY 1168231104530-2, NTLM
                                                192.175.48.1    60 TCP    4271 > dom[illegible] Seq=150 Ack=14 W
                                                192.175.48.1    60 TCP    domain [ACK] Seq=151 Ack=15 Win=16
```

```
+ Frame 11 (203 bytes on wire, 203 bytes captured)
+ Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
+ Internet Protocol, Src: 214.1.101.21 (214.1.101.21), Dst: 192.175.48.1 (192.175.48.1)
+ Transmission Control Protocol, Src Port: 4271 (4271), Dst Port: domain (53), Seq: 1, Ack: 0, Len: 149
- Domain Name System (query)
    Length: 147
    Transaction ID: 0xad3c
  + Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  - Queries
    + 1168231104530-2: type TKEY, class IN
  - Answers
    - 1168231104530-2: type TKEY, class ANY
        Name: 1168231104530-2
        Type: TKEY (Transaction Key)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 87
        Algorithm name: gss.microsoft.com
        Signature inception: Jan 10, 2007 18:01:40.000000000
        Signature expiration: Jan 11, 2007 18:01:40.000000000
        Mode: GSSAPI
        Error: No error
        Key Size: 52
      - Key Data
        - NTLMSSP
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
          + Flags: 0xe208b297
          + Calling workstation domain: NMED
          + Calling workstation name: NHGLISPY
        Other Size: 0
```

TKEY Query; Name is `[digits]-[2|3]`

TKEY Answer Record

TKEY Algorithm `gss.microsoft.com`

NTLMSSP Data

```
0050  33 30 2d 32 00 00 f9 00  01 0f 31 31 36 38 32 33   30-2.... ..116823
0060  31 31 30 34 35 33 30 2d  32 00 00 f9 00 ff 00 00   1104530- 2.......
0070  00 00 00 57 03 67 73 73  09 6d 69 63 72 6f 73 6f   ...W.gss .microso
0080  66 74 03 63 6f 6d 00 45  a5 70 54 45 a6 c1 d4 00   ft.com.E .pTE....
0090  03 00 00 00 34 4e 54 4c  4d 53 53 50 00 01 00 00   ....4NTL MSSP....
00a0  00 97 b2 08 e2 04 00 04  00 30 00 00 00 08 00 08   ........ .0......
00b0  00 28 00 00 00 05 00 93  08 00 00 00 0f 4e 48 47   .(...... .....NHG
```

P: 632 D: 5 M: 0

TCP TKEY Form 1: Key Features

```
    8 2007-01-10 18:01:40.614815 214.1.101.21   192.175.48.1    62 TCP    4271 > domain [SYN] Seq=0 Ack=0 Win=16384
   10 2007-01-10 18:01:40.876805 214.1.101.21   192.175.48.1    60 TCP    4271 > domain [ACK] Seq=1 Ack=0 Win=16560
   11 2007-01-10 18:01:40.877095 214.1.101.21   192.175.48.1   203 DNS    Standard query TKEY 1168231104530-2, NTLM
                                                                        4271 > domain [FIN, ACK] Seq=150 Ack=14 W
                                                                        domain [ACK] Seq=151 Ack=15 Win=16
```

```
Frame 11 (203 bytes on wire, 203 bytes captured)
Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
Internet Protocol, Src: 214.1.101.21 (214.1.101.21), Dst: 192.175.48.1 (192.175.48.1)
Transmission Control Protocol, Src Port: 4271 (4271), Dst Port: domain (53), Seq: 1, Ack: 0, Len: 149
Domain Name System (query)
    Length: 147
    Transaction ID: 0xad3c
  + Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  - Queries
    + 1168231104530-2: type TKEY, class IN
  - Answers
    - 1168231104530-2: type TKEY, class ANY
        Name: 1168231104530-2
        Type: TKEY (Transaction Key)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 87
        Algorithm name: gss.microsoft.com
        Signature inception: Jan 10, 2007 18:01:40.000000000
        Signature expiration: Jan 11, 2007 18:01:40.000000000
        Mode: GSSAPI
        Error: No error
        Key Size: 52
      - Key Data
        - NTLMSSP
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
          + Flags: 0xe208b297
          + Calling workstation domain: NMED
          + Calling workstation name: NHGLISPY
        Other Size: 0
```

```
0050  33 30 2d 32 00 00 f9 00  01 0f 31 31 36 38 32 33   30-2.... ..116823
0060  31 31 30 34 35 33 30 2d  32 00 00 f9 00 ff 00 00   1104530- 2.......
0070  00 00 00 57 03 67 73 73  09 6d 69 63 72 6f 73 6f   ...W.gss .microso
0080  66 74 03 63 6f 6d 00 45  a5 70 54 45 a6 c1 d4 00   ft.com.E .pTE....
0090  03 00 00 00 34 4e 54 4c  4d 53 53 50 00 01 00 00   ....4NTL MSSP....
00a0  00 97 b2 08 e2 04 00 04  00 30 00 00 00 08 00 08   ........ .0......
00b0  00 28 00 00 00 05 00 93  08 00 00 00 0f 4e 48 47   .(...... .....NHG
```

Gateway Address

Workstation Domain (unicode)

Workstation Name (unicode)

P: 632 D: 5 M: 0

TCP TKEY Form 1: Key Features

```
    8 2007-01-10 18:01:40.614815 214.1.101.21   192.175.48.1    62 TCP   4271 > domain [SYN] Seq=0 Ack=0 Win=16384
   10 2007-01-10 18:01:40.876805 214.1.101.21   192.175.48.1    60 TCP   4271 > domain [ACK] Seq=1 Ack=0 Win=16560
   11 2007-01-10 18:01:40.877095 214.1.101.21   192.175.48.1   203 DNS   Standard query TKEY 1168231104530-2, NTLM
                                                192.175.48.1    60 TCP   4271 > domain [FIN, ACK] Seq=150 Ack=14 W
                                                192.175.48.1    60 TCP   domain > 4271 [ACK] Seq=151 Ack=15 Win=16
```

```
⊞ Frame 11 (203 bytes on wire, 203 bytes captured)
⊞ Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
⊞ Internet Protocol, Src: 214.1.101.21 (214.1.101.21), Dst: 192.175.48.1 (192.175.48.1)
⊞ Transmission Control Protocol, Src Port: 4271 (4271), Dst Port: domain (53), Seq: 1, Ack: 0, Len: 149
⊟ Domain Name System (query)
    Length: 147
    Transaction ID: 0xad3c
  ⊞ Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ 1168231104530-2: type TKEY, class IN
  ⊟ Answers
    ⊟ 1168231104530-2: type TKEY, class ANY
        Name: 1168231104530-2
        Type: TKEY (Transaction Key)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 87
        Algorithm name: gss.microsoft.com
        Signature inception: Jan 10, 2007 18:01:40.000000000
        Signature expiration: Jan 11, 2007 18:01:40.000000000
        Mode: GSSAPI
        Error: No error
        Key Size: 52
      ⊟ Key Data
        ⊟ NTLMSSP
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
          ⊞ Flags: 0xe208b297
          ⊞ Calling workstation domain: NMED
          ⊞ Calling workstation name: NHGLISPY
      Other Size: 0
```

Gateway Address

No Private Address Information

Workstation Domain (unicode)

Workstation Name (unicode)

```
0050  33 30 2d 32 00 00 f9 00  01 0f 31 31 36 38 32 33   30-2.... ..116823
0060  31 31 30 34 35 33 30 2d  32 00 00 f9 00 ff 00 00   1104530- 2.......
0070  00 00 00 57 03 67 73 73  09 6d 69 63 72 6f 73 6f   ...W.gss .microso
0080  66 74 03 63 6f 6d 00 45  a5 70 54 45 a6 c1 d4 00   ft.com.E .pTE....
0090  03 00 00 00 34 4e 54 4c  4d 53 53 50 00 01 00 00   ....4NTL MSSP....
00a0  00 97 b2 08 e2 04 00 04  00 30 00 00 00 08 00 08   ........ .0......
00b0  00 28 00 00 00 05 00 93  08 00 00 00 0f 4e 48 47   .(...... .....NHG
```

P: 632 D: 5 M: 0

TCP TKEY Form 2: Windows XP, 2003

```
1 2007-01-08 18:45:37.912301 60.49.189.45      192.175.48.1    274 DNS  Standard query TKEY 4932-ms-7.16548-c2f77
2 2007-01-08 18:45:37.948969 65.114.23.4       192.175.48.1     74 TCP  52852 > domain [SYN] Seq=0 Ack=0 Win=1638
3 2007-01-08 18:45:37.954399 64.254.67.113     192.175.48.1    274 DNS  Standard query TKEY 2840-ms-7.39288-c47f4
4 2007-01-08 18:45:38.[illegible]72.164.150.170 192.175.48.1   274 DNS  Standard query TKEY 3396-ms-7.212141-1bcf
5 2007-01-08 18:45:38.[illegible]               192.175.48.1   274 DNS  Standard query TKEY 3976-ms-7.[illegible]3b740
```

```
Frame 4 (274 bytes on wire, 274 bytes captured)
Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
Internet Protocol, Src: 72.164.150.170 (72.164.150.170), Dst: 192.175.48.1 (192.175.48.1)
Transmission Control Protocol, Src Port: 37083 (37083), Dst Port: domain (53), Seq: 0, Ack: 0, Len: 220
Domain Name System (query)
    Length: 218
    Transaction ID: 0x93f1
  + Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  - Queries
    + 3396-ms-7.212141-1bcfdba.7f1ac758-781e-11db-95ae-0013725454ff: type TKEY, class IN
  - Additional records
    - 3396-ms-7.212141-1bcfdba.7f1ac758-781e-11db-95ae-0013725454ff: type TKEY, class ANY
        Name: 3396-ms-7.212141-1bcfdba.7f1ac758-781e-11db-95ae-0013725454ff
        Type: TKEY (Transaction Key)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 66
        Algorithm name: gss-tsig
        Signature inception: Jan  8, 2007 18:45:37.000000000
        Signature expiration: Jan  9, 2007 18:45:37.000000000
        Mode: GSSAPI
        Error: No error
        Key Size: 40
      - Key Data
        - NTLMSSP
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
          + Flags: 0xe2088297
            Calling workstation domain: NULL
            Calling workstation name: NULL
      Other Size: 0
```

TKEY Query; Name looks like a GUID

TKEY Algorithm `gss-tsig`

NTLMSSP Data: NULL!

```
0000  00 0d 56 71 75 f7 00 08  7c 2c 78 1c 08 00 45 00   ..Vqu... |,x...E.
0010  01 04 40 a7 40 00 74 06  f5 4d 48 a4 96 aa c0 af   ..@.@.t. .MH.....
0020  30 01 90 db 00 35 1a 16  32 fe 97 48 e7 0e 50 18   0....5.. 2..H..P.
0030  ff ff ad 84 00 00 00 da  93 f1 00 00 00 01 00 00   ........ ........
0040  00 00 00 01 09 33 33 39  36 2d 6d 73 2d 37 0e 32   .....339 6-ms-7.2
0050  31 32 31 34 31 2d 31 62  63 66 64 62 61 24 37 66   12141-1b cfdba$7f
0060  31 61 63 37 35 38 2d 37  38 31 65 2d 31 31 64 62   1ac758-7 81e-11db
```

File: "U:/svn/NetSA-2007-49/domain/leftovers.pcap" 4223 KB 00:08:46

P: 15616 D: 15616 M: 0

TCP TKEY Form 2: Windows XP, 2003

```
1 2007-01-08 18:45:37.912301 60.49.189.45     192.175.48.1    274 DNS   Standard query TKEY 4932-ms-7.16548-c2f77
2 2007-01-08 18:45:37.948969 65.114.23.4      192.175.48.1     74 TCP   52852 > domain [SYN] Seq=0 Ack=0 Win=1638
3 2007-01-08 18:45:37.954399 64.254.67.113    192.175.48.1    274 DNS   Standard query TKEY 2840-ms-7.39288-c47f4
4 2007-01-08 18:45:38.[illegible]72.[illegible].150.170  192.175.48.1  274 DNS  Standard query TKEY 3396-ms-7.212141-1bcf
5 2007-01-08 18:45:38.[illegible]                        192.175.48.1  [illegible] Standard query TKEY 3976-ms-[illegible]3b74
```

```
Frame 4 (274 bytes on wire, 274 bytes captured)
Ethernet II, Src: Cisco_2c:78:1c (00:08:7c:2c:78:1c), Dst: DellPcba_71:75:f7 (00:0d:56:71:75:f7)
Internet Protocol, Src: 72.164.150.170 (72.164.150.170), Dst: 192.175.48.1 (192.175.48.1)
Transmission Control Protocol, Src Port: 37083 (37083), Dst Port: domain (53), Seq: 0, Ack: 0, Len: 220
Domain Name System (query)
    Length: 218
    Transaction ID: 0x93f1
  + Flags: 0x0000 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  - Queries
    + 3396-ms-7.212141-1bcfdba.7f1ac758-781e-11db-95ae-0013725454ff: type TKEY, class IN
  - Additional records
    - 3396-ms-7.212141-1bcfdba.7f1ac758-781e-11db-95ae-0013725454ff: type TKEY, class ANY
        Name: 3396-ms-7.212141-1bcfdba.7f1ac758-781e-11db-95ae-0013725454ff
        Type: TKEY (Transaction Key)
        Class: ANY (0x00ff)
        Time to live: 0 time
        Data length: 66
        Algorithm name: gss-tsig
        Signature inception: Jan  8, 2007 18:45:37.000000000
        Signature expiration: Jan  9, 2007 18:45:37.000000000
        Mode: GSSAPI
        Error: No error
        Key Size: 40
      - Key Data
        - NTLMSSP
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
          + Flags: 0xe2088297
            Calling workstation domain: NULL
            Calling workstation name: NULL
      Other Size: 0
```

TKEY Query; Name looks like a GUID

TKEY Algorithm gss-tsig

More Later...

NTLMSSP Data: NULL

```
0000  00 0d 56 71 75 f7 00 08  7c 2c 78 1c 08 00 45 00   ..Vqu... |,x...E.
0010  01 04 40 a7 40 00 74 06  f5 4d 48 a4 96 aa c0 af   ..@.@.t. .MH.....
0020  30 01 90 db 00 35 1a 16  32 fe 97 48 e7 0e 50 18   0....5.. 2..H..P.
0030  ff ff ad 84 00 00 00 da  93 f1 00 00 00 01 00 00   ........ ........
0040  00 00 00 01 09 33 33 39  36 2d 6d 73 2d 37 0e 32   .....339 6-ms-7.2
0050  31 32 31 34 31 2d 31 62  63 66 64 62 61 24 37 66   12141-1b cfdba$7f
0060  31 61 63 37 35 38 2d 37  38 31 65 2d 31 31 64 62   1ac758-7 81e-11db
```

File: "U:/svn/NetSA-2007-49/domain/leftovers.pcap" 4223 KB 00:08:46

P: 15616 D: 15616 M: 0

TCP UPDATEs: Stats

Filter Expression:

```
tcp port 53 and dst net 192.175.48.0/24 and
greater 68
```

TCP Packets Processed	33,407,149	
Workstation, Domain Found	28,583,277	(85.6%)
Null Workstation	4,487,536	(13.4%)
SYN/FIN/RST	336,186	(1.0%)
Malformed Packets	1,331	(0.0%)
TSIG but no NTLM	132	(0.0%)
QR flag set	6	(0.0%)

TCP UPDATEs: Stats (2)

Unique Entries (gateway, domain, workstation)		
Total	279,916	
NaMeX	44,286	(15.8%)
WIDE	235,635	(84.2%)
Overlap	5*	(0.0%)
Unicode Domains	1,099	(2.4%)
Unicode Workstations	4,675	(2.6%)

*Same sources as for UDP UPDATEs

TCP UPDATEs: Most Popular Gateways

Clients	Gateway	Owner
2,632	202.42.255.254	Singapore General Hospital
2,452	219.81.16.30	Taiwan Fixed Network CO.,LTD.
2,130	210.128.214.254	Nitori Co., Ltd. (furniture retailer)
1,491	202.214.81.194	West Nippon Expressway Company Limited
1,222	60.48.15.219	Telekom Malaysia Berhad
988	60.48.19.195	Telekom Malaysia Berhad
799	66.77.33.167	Pro Furniture Row LLC
791	220.130.69.5	Chunghwa Telecom Co.,Ltd (Taiwan)
754	219.188.194.254	Japan nation-wide Network of SOFTBANK BB CORP
639	211.23.62.187	Chunghwa Telecom Co.,Ltd (Taiwan)

Similar to UDP gateways, except more corporate networks

Client Workstation Counts

Clients	Domain	Gateway	Owner
1,908	SGHAD	202.42.255.254	Singapore General Hospital
1,483	WEST	202.214.81.194	West Nippon Expressway Company Ltd
879	AMBANKGROUP	60.48.15.219	Telekom Malaysia Berhad
780	FRSALES	66.77.33.167	Pro Furniture Row LLC
768	CSH	220.130.69.5	Chunghwa Telecom Co.,Ltd (Taiwan)
743	BB	219.188.194.254	Japan nation-wide SOFTBANK BB
697	AMBANKGROUP	60.48.19.195	Telekom Malaysia Berhad
638	KUOZUI	211.23.62.187	Chunghwa Telecom Co.,Ltd (Taiwan)
608	KUOZUI	220.130.36.130	Chunghwa Telecom Co.,Ltd (Taiwan)
602	KUOZUI	61.222.92.211	Chunghwa Telecom Co.,Ltd (Taiwan)

Most Popular Workstation Name

Clients	Private /24
6,065	SERVER
873	SERVER01
764	SERVER1
329	SERVER02
311	NTSERVER
299	SERVER2000
299	DHCP
283	FILESERVER
281	MAIL
273	BBSM52

2.2%

Clients	Private /24
248	SERVER2
222	W2KSERVER
205	EXPRESS5800
191	OFFICE
182	SV01
154	SV1
152	SCOTT
143	SAPDSVR
140	MARK
132	SERVER2K

Most Popular Domain Name

Gateways	Private /24
11,039	WORKGROUP
1,961	DOMAIN
670	STCHARLES
593	SEBRING
547	POLARBEAR
512	SALEMSCHOOLS
443	YDOADS
425	NRCN
425	MSHOME
422	EAST_LIVERPOOL

11.3%

*Counts represent the number of *Gateways* using a particular domain name

Data Analysis:

TSIG Names

TSIG Names: Two Formats (revisited)

- Windows 2000

  962072674322-2

  1065151889426-2

  3985729650706-2

  7627861917714-3

  6923487281170-2

  1047972020242-2

  1013612281874-3

- Windows 2003/XP

  2988-ms-7.61440-19b1c78f.74bae630-9d13-11db-61bb-0010180dacbc

  1920-ms-7.30789-7f24b0d.73103774-9fc7-11db-5eb2-001321c84d09

  928-ms-7.213083-c2aa1a4.c9fb0b8a-9f23-11db-a1b2-0002b3c712be

  3680-ms-7.54569-46d9335a.38cc9ec8-962f-11db-b6a7-001143d9fb76

  2036-ms-7.255072-7d2a7998.28bb8cee-8de5-11db-d1b7-0002a5f0d4b6

  1332-ms-7.42113-3f1d5548.f481e320-975c-11db-5b86-0014220c67ee

  3408-ms-7.77054-2d821f07.d01c7e98-9a0c-11db-fe80-000bcd9a9627

TSIG Names: Windows 2000 Format

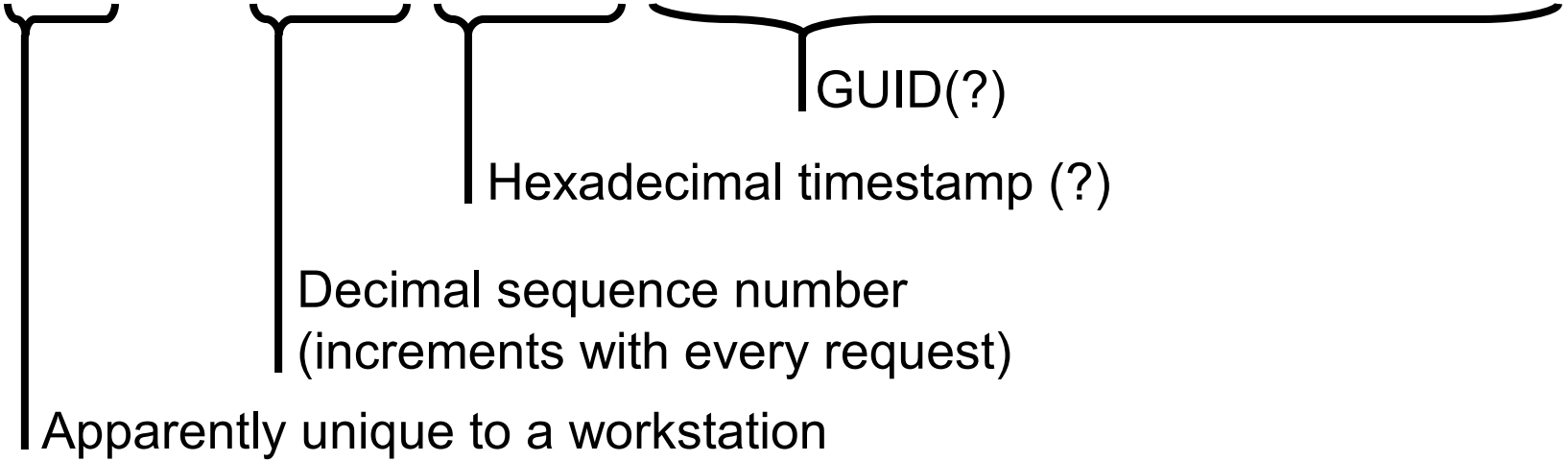
- Arrive in triplets
  - —Same root; one “-3” suffix, then two “-2” suffix
- Convert root to hex:

```
962072674322  = 00E0 0000 0012
1065151889426 = 00F8 0000 0012
3985729650706 = 03A0 0000 0012
7627861917714 = 06F0 0000 0012
6923487281170 = 064C 0000 0012
1047972020242 = 00F4 0000 0012
1013612281874 = 00EC 0000 0012
```

  - —The last for bytes do actually changed *occasionally*
  - —Two bytes are not enough for a fingerprint

TSIG Names: Windows 2003 Format

```
2988-ms-7. 61440-19b1c78f.74bae630-9d13-11db-61bb-0010180dacbc
1920-ms-7. 30789- 7f24b0d.73103774-9fc7-11db-5eb2-001321c84d09
 928-ms-7.213083- c2aa1a4.c9fb0b8a-9f23-11db-a1b2-0002b3c712be
3680-ms-7. 54569-46d9335a.38cc9ec8-962f-11db-b6a7-001143d9fb76
2036-ms-7.255072-7d2a7998.28bb8cee-8de5-11db-d1b7-0002a5f0d4b6
1332-ms-7. 42113-3f1d5548.f481e320-975c-11db-5b86-0014220c67ee
3408-ms-7. 77054-2d821f07.d01c7e98-9a0c-11db-fe80-000bcd9a9627
```



Can the GUID be used to uniquely identify NATd machines?

TSIG XP/2003 TSIG Stats

TSIG Names:		
TSIG Packets Processed	34,651,194	
Windows 2000 Format	29,881,014	(86.2%)
Windows XP/2003 Format	4,768,781	(13.8%)
XP/2003 GUIDS:		
Unique GUIDs	1,508*	
GUIDS with Multiple Gateways	64**	(4.2%)

* *Assuming the GUID is unique to the machine, this equates to 3162 TSIG packets per machine over 48 hours. With 3 retries per update,* ***each machine retries roughly every 3 minutes****.*

** *Gateways addresses these GUIDs were all registered to the same owners.*

Anomalies

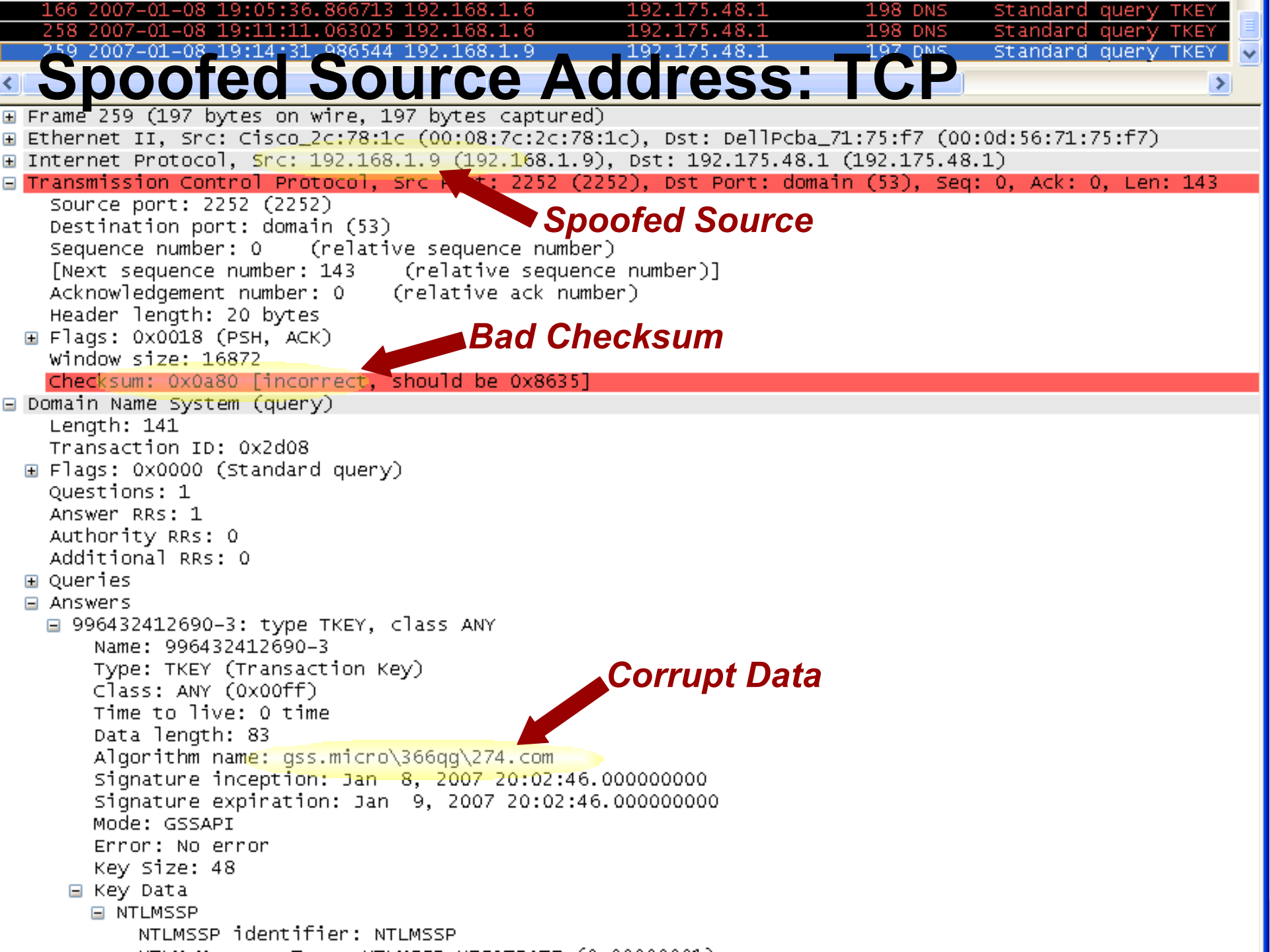
Anomalies: "Spoofed" Source Address

Gateway (source) address within RFC1918 space

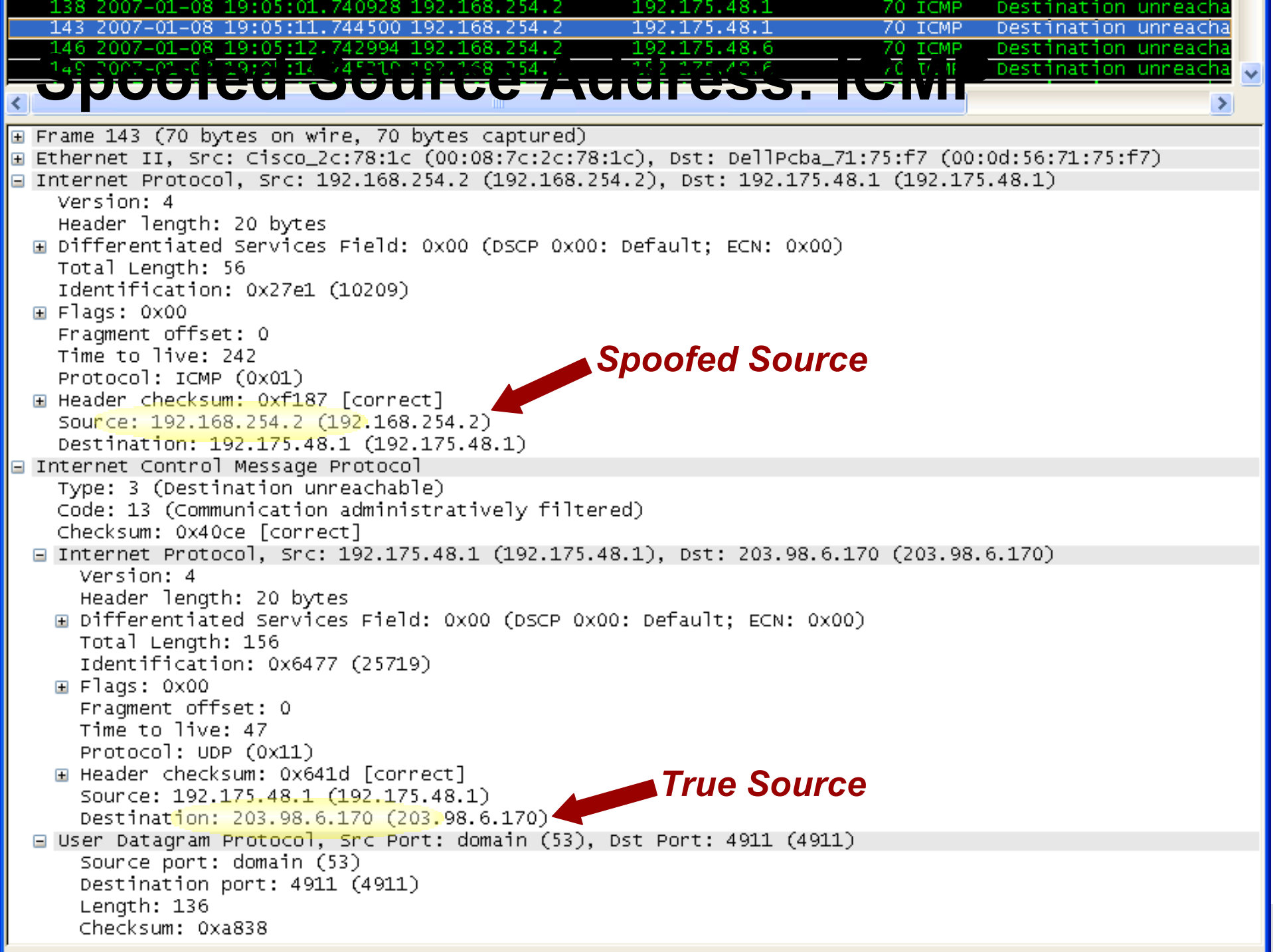
- Over 2000 events in UDP UPDATEs alone
- The spoofed IP is not always the same as the UPDATE
- Mostly SOA, PTR queries
  - —Some TCP SYNs
  - —One set of ICMP "filtered" replies
  - —Even one set of TCP data (TSIG) packets (!)

WIDE replied (didn't check NaMeX)

Spoofed Source Address: TCP



Spoofed Source Address: ICMP



Anomalies: "Spoofed" Source Address

Probably broken NATs and corruption

- (or could this be crafted/malicious?)
- Interesting, but not huge

Conclusions and Future Work

Data Extfiltration via AS112

Problem Statement: What internal network topology data is exposed to the public Internet?

- Gateway address
- Private Address
- Private Name
- Windows Domain
- Windows Workstation Name

Recommendations

What are the prioritized preferred solutions?

- Make your DNS server authoritative for ***all*** RFC1918 PTR zones
- Create site-local dead-end SOA entries for RFC1918 PTR zones (?)
- Create site-local dead-end DNS entries for prisoner.iana.org, blackhole-1,2.iana.org (?)
- Block all outbound traffic 192.175.48.0/24 (?)
- Reroute AS112 traffic internally (?)

Best Publication Route?

Analysis of AS112 Traffic

Sid Faber
Network Situational Awareness Group
sfaber@cert.org