



INSIDE
PRODUCTS

Forensics for IPv6

Nalini Elkins
Inside Products, Inc.



INSIDE
PRODUCTS

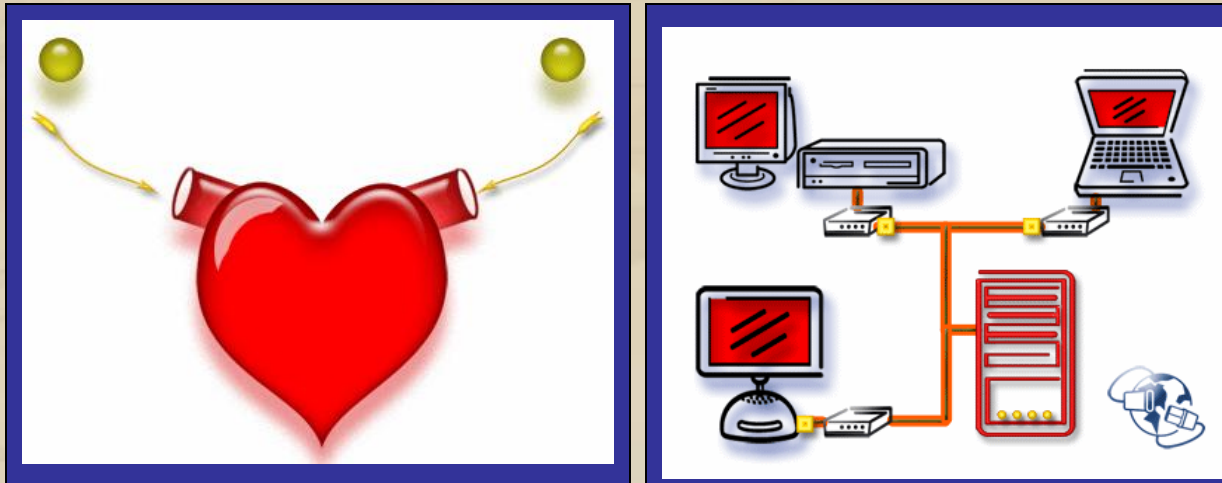
Thinking Inside the Box

Inside Products, Inc.

sales@insidestack.com

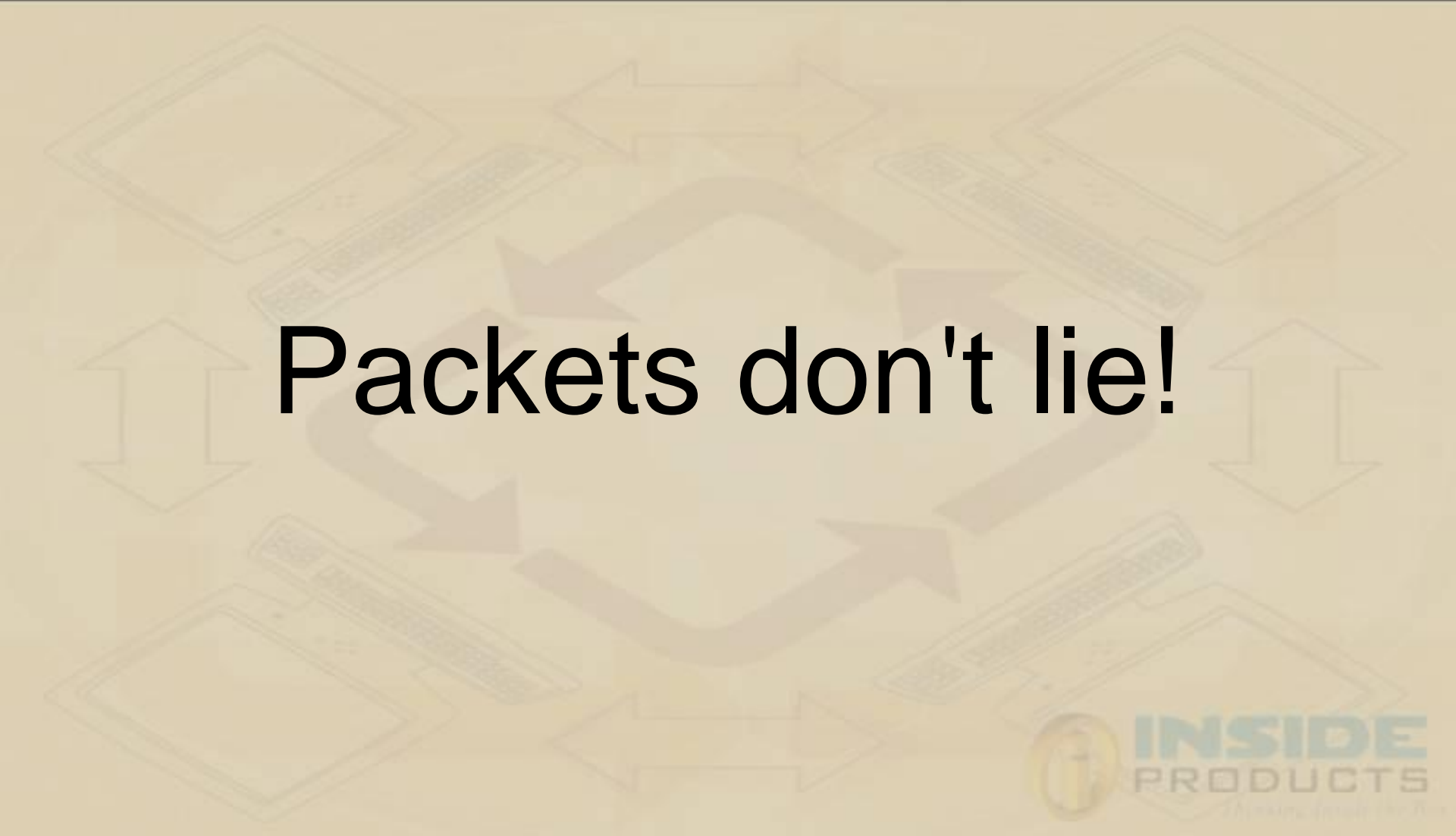
(831) 659-8360

Why Forensics? Reducing Risk



- Problems on networks are inevitable (low throughput, poor response time, network overhead, excessive server CPU usage).
- The only question is how quickly the problems can be resolved. Sometimes the best, the only way, is to take a trace.

Why trace?



Packets don't lie!

Let's look at a packet

- First, we do some analysis of it:
- A DNS request was found at packetid: 4088.
- The original query was a type: AAAA which returns a 128-bit IPv6 address.
- The resource to be resolved was: www.facebook.com.
- The DNS response had no error.
- The DNS response found 1 answer(s). As follows:
- IPv6 Address:2620::1c00:0:face:b00c:0:2
- TimeToLive:0 Hours 0 Minutes, 29 Seconds.
- The response time for the DNS request / response was: 0.023.376.

```
⊕ Frame 4094: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
⊕ Ethernet II, Src: Cisco_b6:87:c0 (00:08:7c:b6:87:c0), Dst: Xensourc_68:72:c0 (00:16:3e:68:72:c0)
⊕ Internet Protocol, Src: 8.8.8.8 (8.8.8.8), Dst: 208.111.39.67 (208.111.39.67)
⊕ User Datagram Protocol, Src Port: domain (53), Dst Port: 35146 (35146)
⊖ Domain Name System (response)
  \[Request In: 4088\]
  [Time: 0.023099000 seconds]
  Transaction ID: 0x2c4b
⊕ Flags: 0x8180 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
⊖ Queries
  ⊕ www.facebook.com: type AAAA, class IN
⊖ Answers
  ⊖ www.facebook.com: type AAAA, class IN, addr 2620:0:1c00:0:face:b00c:0:2
    Name: www.facebook.com
    Type: AAAA (IPv6 address)
    Class: IN (0x0001)
    Time to live: 29 seconds
```

WireShark provides a good breakout. Tracing gives an understanding of protocols.

Let's look at a typical problem



Business partner is having throughput problems with a new application.

Network Viewpoint

- Network technician says that the window size is set less than 4k but the bytes in flight are only 1k!
- So “obviously” any delays are due to the design of the application.

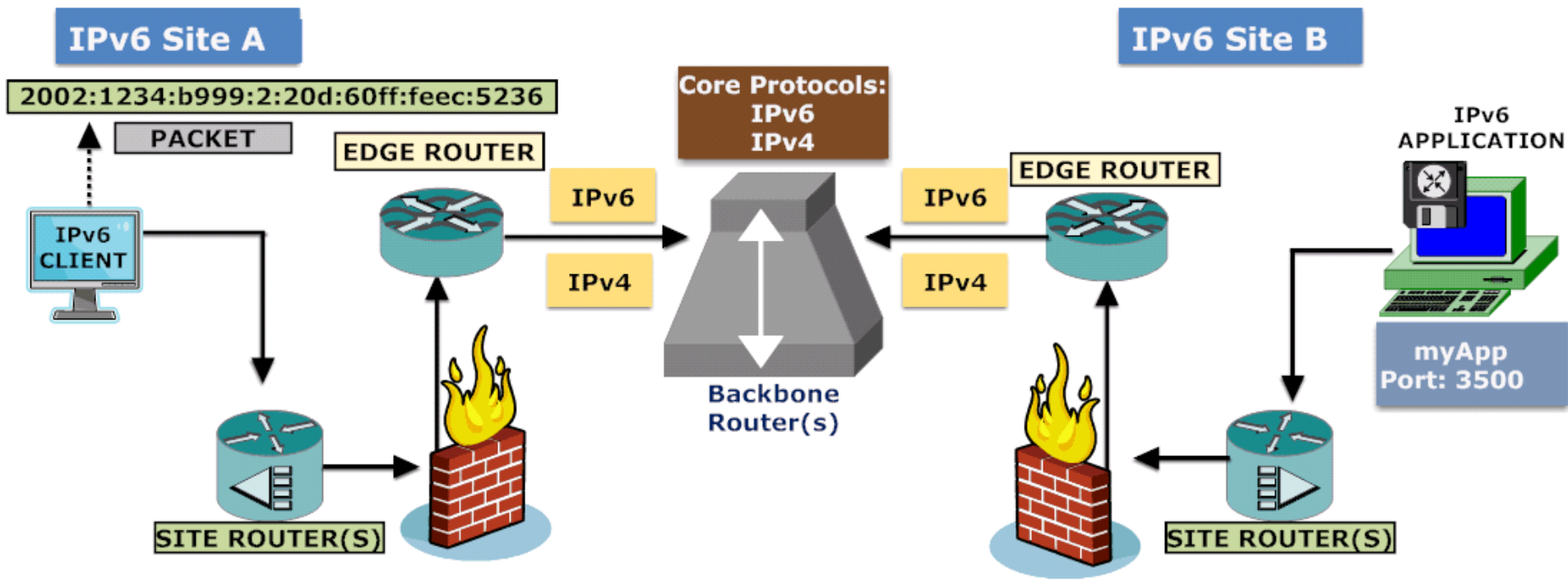
Bytes In Flight???

- Speedometer in car may say you can go up to 150 mph – this is congestion window
- How fast are you actually going? Maybe 60 mph – this is bytes in flight.

Wait a minute!

- But, this is an IPv4 problem!
- Can the same thing happen in IPv6 networks?

So, there are no apps in IPv6?



Can the same thing happen in IPv6 networks?

What is different with IPv6?

- Diagnostics and troubleshooting is different
 - Tunneled packets
 - Understanding of addressing (ULA, LinkLocal, etc)
 - DNSv6,
 - DHCPv6,
 - Neighbor Discovery...

Now, we come to Forensics

- What has to be calculated? Network
 - Congestion Window
 - Bytes in Flight
 - Bytes per second
 - Packets per second
- What has to be calculated? Application
 - Find if there is delay in responding

Calculate Throughput

IP
PROBLEM FINDER

Show TCP Address List
Sort Order : Bytes per Second Descending
Showing Entries : 1 - 10

	Source Address	Source Port	Destination Address	Destination Port	IP Protocol	Connection Time (ss.milli.micro)	Total Packets	Throughput Packets Per Second	Total Data Bytes	Throughput Bytes Per Second
1	2001: [redacted] :F001	1031	2001: [redacted] :F001	1032	IPv6	0.110.794	4 (1.44%)	4	344 (2.5%)	344
2	172. [redacted] 222	230	172. [redacted] 1	1184	IPv4	85.942.273	118 (42.75%)	1	11K (85.06%)	137
3	2001: [redacted] :F001	21	2001: [redacted] :F001	1030	IPv6	13.892.775	11 (3.98%)	0	350 (2.54%)	26
4	2001: [redacted] :F001	21	2001: [redacted] :F001	1029	IPv6	11.381.704	8 (2.89%)	0	212 (1.54%)	19
5	172. [redacted] ,1	1184	172. [redacted] 222	230	IPv4	84.926.078	108 (39.13%)	1	1K (7.75%)	12
6	2001: [redacted] :F001	1029	2001: [redacted] :F001	21	IPv6	11.381.718	10 (3.62%)	0	34 (0.24%)	3
7	2001: [redacted] :F001	1030	2001: [redacted] :F001	21	IPv6	13.892.794	13 (4.71%)	1	47 (0.34%)	3
8	2001: [redacted] :F001	1032	2001: [redacted] :F001	1031	IPv6	0.110.801	4 (1.44%)	4	0 (0.0%)	0
-	-	-	-	-	-	276	13K	-	-	-

- BTW, also allows you to answer is IPv6 faster or slower?

Throughput – both ways!

- **First side:**
- The total connection time for 2001:DB8::222:F001 port:21 to 2001:DB8::222:F001 port:1030 was 13 seconds, 892 milliseconds, 775 microseconds.
- The bytes per second sent by this half of the connection was 26.
- The minimum bytes in flight sent by this half of the connection was 0.
- The average bytes in flight sent by this half of the connection was 39.
- The maximum bytes in flight sent by this half of the connection was 123.

Now, the other way

- **Second side:**
- The total connection time for 2001:DB8::222:F001 port:1030 to 2001:DB8::222:F001 port:21 was 13 seconds, 892 milliseconds, 794 microseconds.
- The bytes per second sent by this half of the connection was 3.
- The minimum bytes in flight sent by this half of the connection was 0.
- The average bytes in flight sent by this half of the connection was 3.
- The maximum bytes in flight sent by this half of the connection was 15.

Tunneled Packets

Frame #80

Time: Sunday, 6 February 2011 08:42:33.694462

IP Header:

Version: 4

IP Header Length: 20 bytes

Type of Service: 0x00 Precedence: Routine, Delay: Normal, Throughput:
Normal, Reliability: Normal

Total Length: 108

Identification: 0x469c (18076)

Flags: 0x00 (Reserved bit: Not set. Don't fragment: Not set. More
fragments: Not set.)

Fragment offset: 0

Time to Live: 128

Protocol: UDP(0x11)

Header Checksum: 0xb817

Source Address: 192.168.1.101

Destination Address: 202.169.175.22

UDP Header

UDP Header:

Source Port: 1435

Destination Port: 3653

Length: 88

Checksum: 0x154a

UDP Header data:

059b0e45 0058154a

***** Tunneled Protocol: Tunnel Broker

IP Header:

Version: 6

IPv6 Header

IP Header:

Version: 6

Priority: 0 (uncharacterized traffic)

Flow Label: 0x0

Payload Length: 40 octets

Next Header: ICMP for IPv6 (0x3a)

Next Header: ICMP for IPv6 (0x3a)

Hop Limit: 128

Source Address: 2001:c08:3700:ffff::10:f88e

Destination Address: 2001:200:dff:fff1:216:3eff:feb1:44d7

ICMPv6 Header:

Type: 128 Echo Request

ICMPv6 Header and Data

ICMPv6 Header:

Type: 128 Echo Request

Checksum: 0xc468

Identifier: 0x0000

Sequence Number: 0x0058

Other data:

00586162 63646566 6768696a 6b6c6d6e 6f707172

(Xabcdefgh ijklmnopqr)

73747576 77616263 64656667 6869

(stuvwabcde fghi)

Analyze Neighbor Discovery

Show Detailed ICMP Analysis

Trace File: sample022

Showing Entries : 1 -10

IP
PROBLEM FINDER

	Addresses	Error Code	Events
<p>1</p> <p>2607:F740::3F:216:3EFF:FE68:72C0 Port:0 FE80::20C:CFFF:FEAE:300A Port:0</p>	<p>302</p>	<p>Messages Sent</p> <ul style="list-style-type: none"> • ICMP message(s) of type:NEIGHBOR ADVERTISEMENT from 2607:F740::3F:216:3EFF:FE68:72C0 found. The number of packets sent is: 1. The number of bytes sent is: 40. • The source IP (2607:F740::3F:216:3EFF:FE68:72C0) type is: Global Unicast. • The destination IP (FE80::20C:CFFF:FEAE:300A) type is: Link Local. • The total number of ICMP packets in this trace were 33. The percent of NEIGHBOR ADVERTISEMENT packets sent by 2607:F740::3F:216:3EFF:FE68:72C0 were 3.03%. • The total number of bytes for ICMP packets in this trace were 7960. The percent of bytes sent for NEIGHBOR ADVERTISEMENT packets by 2607:F740::3F:216:3EFF:FE68:72C0 port: 0 were 0.5%. <p>NEIGHBOR ADVERTISEMENT Analysis</p> <ul style="list-style-type: none"> • A Neighbor Advertisement packet may be in response to a Neighbor Solicitation packet or it may be sent at regular intervals. • The Neighbor Advertisement packet is letting for any active devices on the same link (router) know that it is active. • This Neighbor Advertisement packet may be a part of the stateless autoconfiguration process if this set of packets is sent at the initialization of this device. 	
		<p>Messages Sent</p>	

DNS Analysis

- DNS is one of the first things to be converted and tested.
- What kind of queries are going out?
- Following are from traces captured on World IPv6 Day, 2011.

DNSv6 Performance

IP
PROBLEM FINDER

Show DNS Traffic / Error Analysis
Trace File:sample022

Total Packets All DNS	Total Bytes All DNS	Average Data Length All DNS	Minimum DNS Response Time All DNS	Average DNS Response Time All DNS	Maximum DNS Response Time All DNS
496	27,117	79	0.000.000	0.058.815	1.183.995

Total DNS Requests	Total Bytes for DNS Requests	Average Request Data Length for DNS Requests
374	15,841	36

- Analysis of DNSv6 can be quite difficult.
- How many packets were sent?
- How quickly were they sent?

Analyze DNS Requests

Show DNS Requests

Sort Order : Packet Number

Showing Entries : 1 - 10

Trace File:sample022

IP
PROBLEM FINDER

Source Address	Source Port	Destination Address	Destination Port	Transaction ID	Flags	Resource	Type	Data Length
208.111.39.174	5353	224.0.0.251	5353	0x0000	0x	240.92.56.213.in-addr.arpa	PTR	44
2607:F740::3F:1216:3EFF:FE7F:1C46	5353	FF02::FB	5353	0x0000	0x	245.2.38.222.in-addr.arpa	PTR	51
208.111.34.12	5353	224.0.0.251	5353	0x0000	0x	245.2.38.222.in-addr.arpa	PTR	43
2607:F740::3F:0:0:0:EF6	5353	FF02::FB	5353	0x0000	0x	240.92.56.213.in-addr.arpa	PTR	52
208.111.39.39	5353	224.0.0.251	5353	0x0000	0x	240.92.56.213.in-addr.arpa	PTR	44
208.111.34.12	5353	224.0.0.251	5353	0x0000	0x	245.2.38.222.in-addr.arpa	PTR	43
2607:F740::3F:1216:3EFF:FE7F:1C46	5353	FF02::FB	5353	0x0000	0x	245.2.38.222.in-addr.arpa	PTR	51
208.111.34.95	5353	224.0.0.251	5353	0x0000	0x	245.2.38.222.in-addr.arpa	PTR	43
208.111.39.179	5353	224.0.0.251	5353	0x0000	0x	240.92.56.213.in-addr.arpa	PTR	44
2607:F740::3F:0:0:0:EF6	5353	FF02::FB	5353	0x0000	0x	240.92.56.213.in-addr.arpa	PTR	52

Analyze DNS Responses

IP
PROBLEM FINDER

Show DNS Responses
 Sort Order : Packet Number
 Showing Entries : 1 -10
 Trace File:sample022



Source Address	Source Port	Destination Address	Destination Port	Transaction ID	Flags	Resource	Type	Data Length	Error Code	Error Message	Response Time (ss.milli.micro)	Request Packet
8.8.8.8	53	208.111.39.67	60591	0xd278	0x818	insidestack.tcpproblemfinder.com	A	121	3	Name Error	0.171.255	1072
8.8.8.8	53	208.111.39.67	49190	0x828e	0x818	start.ubuntu.com	AAAA	95	0		0.023.228	1104
8.8.8.8	53	208.111.39.67	48918	0xe897	0x818	start.ubuntu.com.tcpproblemfinder.com	AAAA	123	3	Name Error	0.151.750	1106
8.8.8.8	53	208.111.39.67	54244	0xd022	0x818	start.ubuntu.com	A	82	0		0.022.879	1110
8.8.8.8	53	208.111.39.67	33871	0x64d4	0x818	help.ubuntu.com	AAAA	94	0		0.023.246	1160
8.8.8.8	53	208.111.39.67	35277	0xfa87	0x818	shop.ubuntu.com	AAAA	94	0		0.022.962	1161
8.8.8.8	53	208.111.39.67	43319	0xd2a5	0x818	www.google.com	AAAA	80	0		0.028.226	1159
8.8.8.8	53	208.111.39.67	49027	0x54e2	0x818	www.google.com	A	132	0		0.028.870	1168
8.8.8.8	53	208.111.39.67	34434	0xe4ab	0x818	www.ubuntu.com	AAAA	93	0		0.022.506	1172
8.8.8.8	53	208.111.39.67	34434	0xe4ab	0x818	www.ubuntu.com	AAAA	93	3	Name Error	0.126.825	1165

Analyze DNS responses and errors to see exactly what happened.

See if A and AAAA queries are being done for IPv4 or IPv6 transactions.

Show Detailed DNS Analysis
Trace File: s22j
Source or Destination Port:34191
Showing Entries : 1 -10



	Addresses	Error Code	Events
1	8.8.8.8 Port:53 208.111.39.67 Port:34191	603	DNS Analysis <ul style="list-style-type: none">• A DNS request was found at packetid: 1177.• The transaction ID was: 0xb427.• The application for 8.8.8.8 is: Domain Name Server.• At packetid, 1193, a DNS response from 8.8.8.8 port:53 was found.• The data length for the DNS response was: 121.• The original query was a type: AAAA.• This performs the function: Returns a 128-bit IPv6 address.• The resource to be resolved was: www.ubuntu.com.tcpproblemfinder.com.• The response time for the DNS request / response was: 0.140.683.• The DNS response received an error.• The error code indicates: This is an unrecoverable error. A Name Error was encountered. This code is meaningful only for responses from an authoritative name server. This code signifies that the domain name referenced in the query does not exist. This error is defined in RFC 1035 as error code 3.• No answers were found.

Conclusion

- Forensics is more important than ever!
- Get ready **BEFORE** the real problems hit.