DMZ Network Visibility with Wireshark

June 15, 2010

Ashok Desai

Senior Network Specialist | Intel Information Technology

SHARKFEST **'10**
Stanford University
June 14-17, 2010

Outline

Presentation Objective

DMZ Overview / Challenges

Case Study

Summary

SHARKFEST '10

Presentation Objective

Share challenges faced when DMZ network visibility is needed

Share methods to help overcome these challenges

Share Wireshark capabilities that are useful for analyzing DMZ traffic

SHARKFEST '10

DMZ Overview

DMZ (Demilitarized Zone) Network

“a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network”

“a network, not part of Internet or Intranet”

Typical DMZ Services

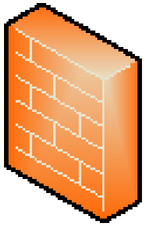
- Firewall
- Load Balancer
- Reverse Proxy

SHARKFEST ‘10

Firewall

Firewall

Designed to block unauthorized access while permitting authorized communications



Types:

1. Network layer firewall
2. Application layer firewall

SHARKFEST '10

Firewall Types

Network layer firewall

- Will not allow packets to pass through the firewall unless they match the established rule set
- Includes source and destination IP address, UDP or TCP ports

Application layer firewall

- Application firewalls can prevent all unwanted outside traffic from reaching protected machines
- Work at the application layer of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic)

Can be single appliance or separate appliances

SHARKFEST '10

Firewall Functionality

- Network and Port Address Translation
  - Hides the true address of protected hosts
- Load Balancer
  - Provides redundancy & load balancing requests

- Challenges for Protocol Analysis
  - Tracking the user task's level traffic
    - Source IP and TCP port number can changes when they pass through

SHARKFEST '10

Load Balancer

Load Balancer

A technique to distribute workload evenly across two or more computers, network links, CPUs, hard drives, or other resources

Can be software or appliance based

Types of Load Balancers*

1. Direct Routing (DR)
2. Network Address Translation (NAT)
3. Source Network Address Translation (SNAT)
4. Transparent Source Network Address Translation (SNAT-TPROXY)
5. SSL Termination or Acceleration (SSL) with or without TPROXY

*- Source http://loadbalancer.org

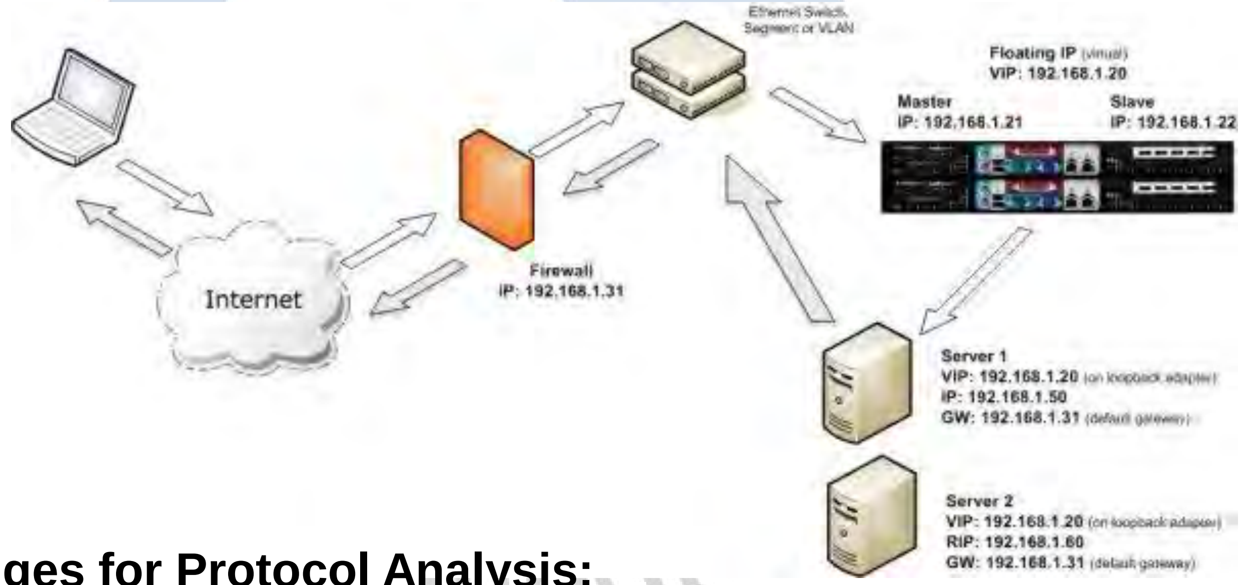
Load Balancer: Type 1

Direct Routing (DR) load balancing method

The virtual IP address is shared by real servers and the load balancer

Load balancer selects on real server, directly forwards to real server

Real server process the request locally and sends response packet directly to client


Ethernet Switch, Segment or VLAN
Floating IP (virtual)
VIP: 192.168.1.20
Master
IP: 192.168.1.21
Slave
IP: 192.168.1.22
Internet
Firewall
IP: 192.168.1.31
Server 1
VIP: 192.168.1.20 (on loopback adapter)
IP: 192.168.1.50
GW: 192.168.1.31 (default gateway)
Server 2
VIP: 192.168.1.20 (on loopback adapter)
RIP: 192.168.1.60
GW: 192.168.1.31 (default gateway)

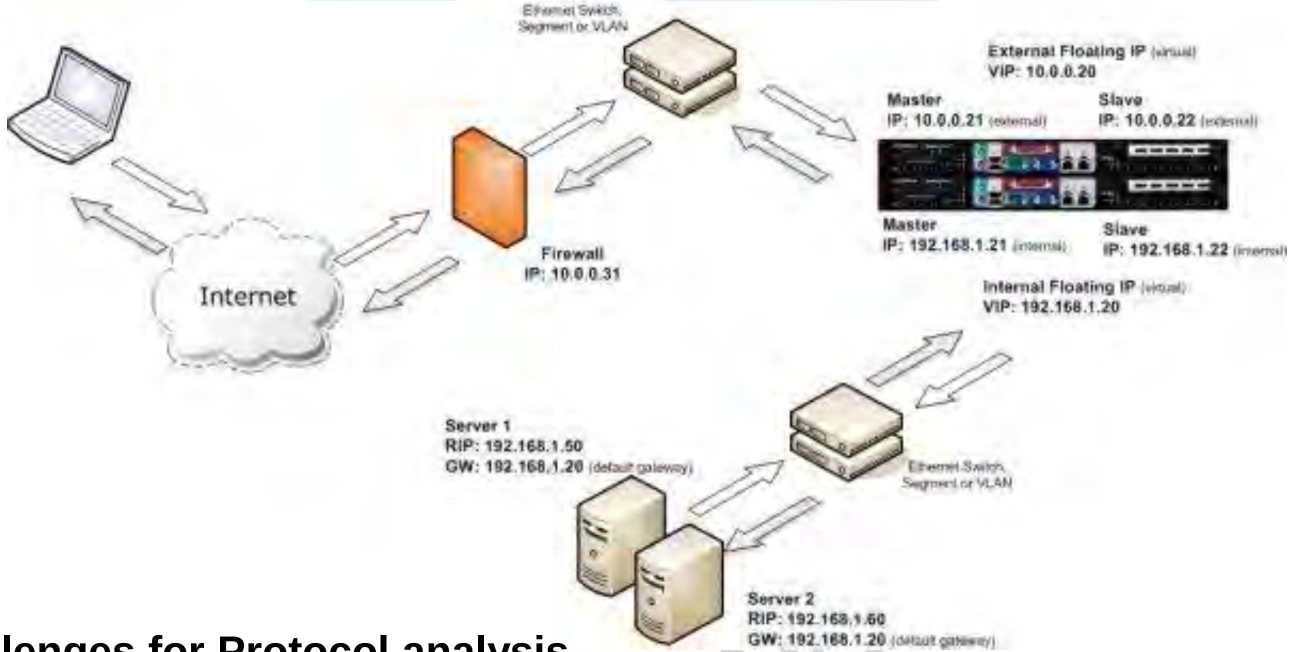
Challenges for Protocol Analysis:

-

Load Balancer: Type 2

Network Address Translation (NAT) load balancing method

- A two arm infrastructure with an internal and external subnet to carry out the translation
- Appliance becomes the default gateway for the real servers
- Load balancer translates all requests from the external virtual server to the internal real servers.


Ethernet Switch, Segment or VLAN
External Floating IP (virtual)
VIP: 10.0.0.20
Master
IP: 10.0.0.21 (external)
Slave
IP: 10.0.0.22 (external)
Master
IP: 192.168.1.21 (internal)
Slave
IP: 192.168.1.22 (internal)
Internal Floating IP (virtual)
VIP: 192.168.1.20
Internet
Firewall
IP: 10.0.0.31
Server 1
RIP: 192.168.1.50
GW: 192.168.1.20 (default gateway)
Ethernet Switch, Segment or VLAN
Server 2
RIP: 192.168.1.60
GW: 192.168.1.20 (default gateway)

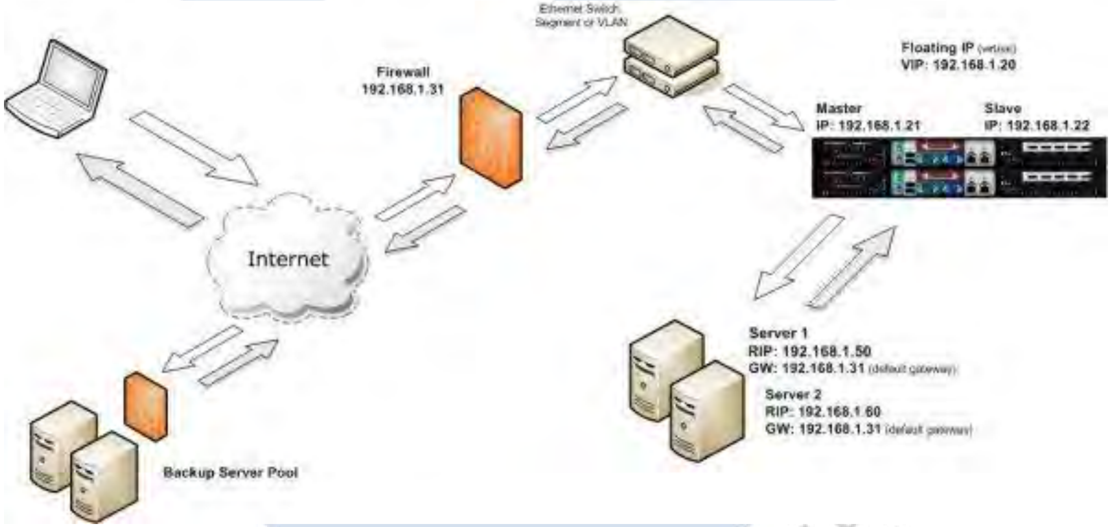
Challenges for Protocol analysis

Load Balancer: Type 3

Source Network Address Translation (SNAT) load balancing method

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer

Load balancer handles cookie insertion



Challenges for Protocol Analysis:

➢

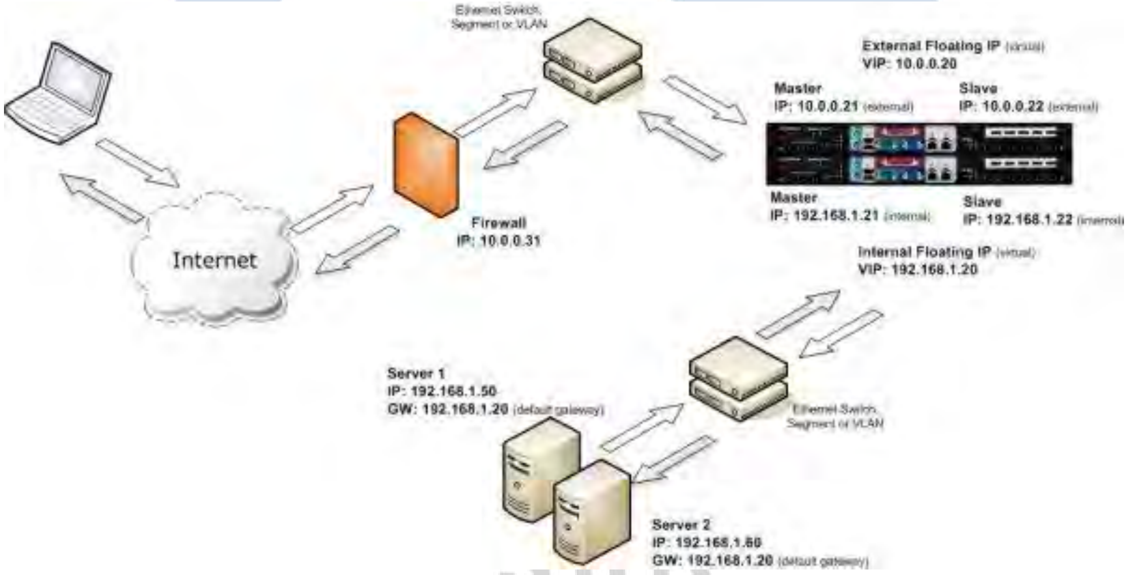
Load Balancer: Type 4

Transparent Source Network Address Translation (SNAT-TPROXY) load balancing method

Source address of the client is a requirement

SNAT acts as a full proxy but in TPROXY mode all server traffic must pass through the load balancer

The real servers must have their default gateway configured to point at the load balancer

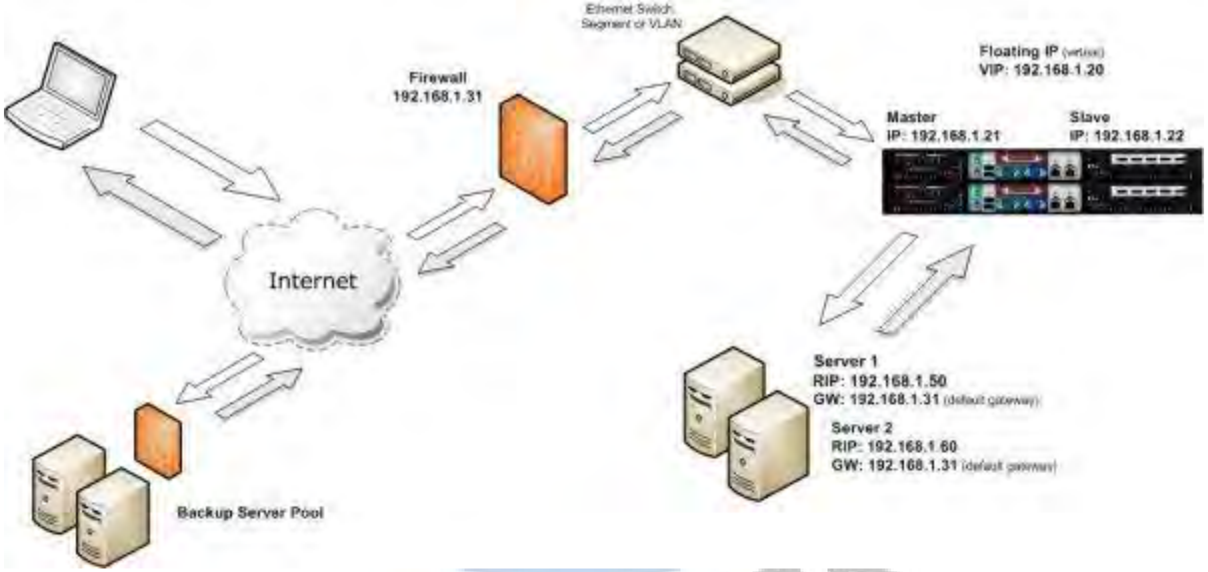

Ethernet Switch, Segment or VLAN
External Floating IP (virtual)
VIP: 10.0.0.20
Master
IP: 10.0.0.21 (external)
Slave
IP: 10.0.0.22 (external)
Master
IP: 192.168.1.21 (internal)
Slave
IP: 192.168.1.22 (internal)
Internal Floating IP (virtual)
VIP: 192.168.1.20
Internet
Firewall
IP: 10.0.0.31
Server 1
IP: 192.168.1.50
GW: 192.168.1.20 (default gateway)
Ethernet Switch, Segment or VLAN
Server 2
IP: 192.168.1.60
GW: 192.168.1.20 (default gateway)

Challenges for Protocol Analysis:

-

Load Balancer: Type 5

SSL Termination or Acceleration (SSL) with or without TPROXY



Challenges for Protocol Analysis:

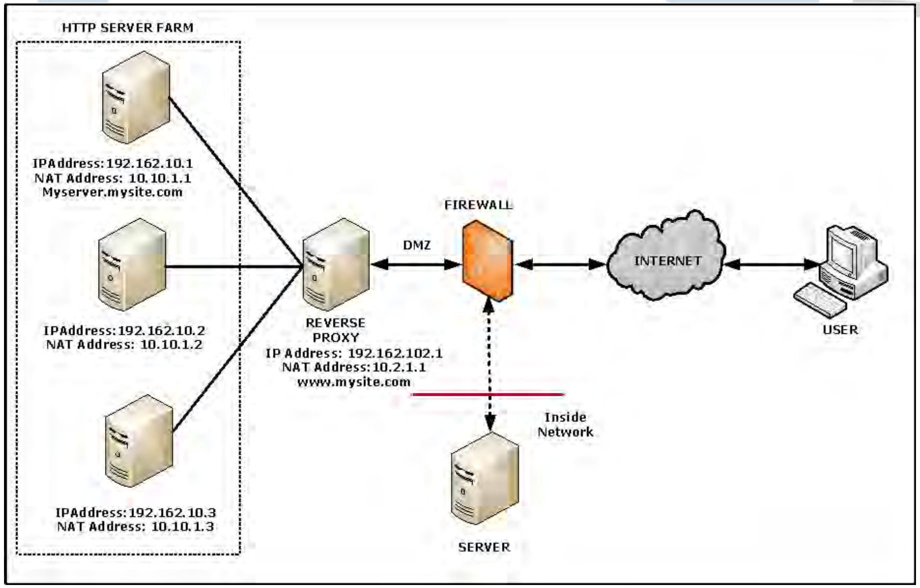
-

SHARK

Reverse Proxy

Reverse Proxy

- Acts as a gateway to an HTTP server or HTTP server farm by acting as the final IP address for requests from the outside
- Dispatches in-bound network traffic to a set of servers, presenting a single interface to the caller
- Uses NAT or PAT to accomplish this



Reverse Proxy

Challenges for Protocol Analysis

- Tracking the user task's traffic across DMZ appliances
  - IP Address and port number will changes once it passes through the reverse proxy
- URL may be different at each DMZ appliance

DMZ Network Challenges – Summary

DMZ network analysis can be challenging:

- Encrypted traffic
- Changing IP addresses and port numbers across:
  - Load Balancer
  - Reverse Proxy
  - Firewall
- Traffic can be difficult to correlate across tiers

SHARKFEST '10

HTTP Protocol Overview

- Compliments protocol analysis efforts
  - HTTP is a request-response standard typical of client-server computing
  - Provides response when there is successful or unsuccessful event
    - Helps to guide where could be cause of issue

Outline

Presentation Objective

DMZ Overview / Challenges

Case Study

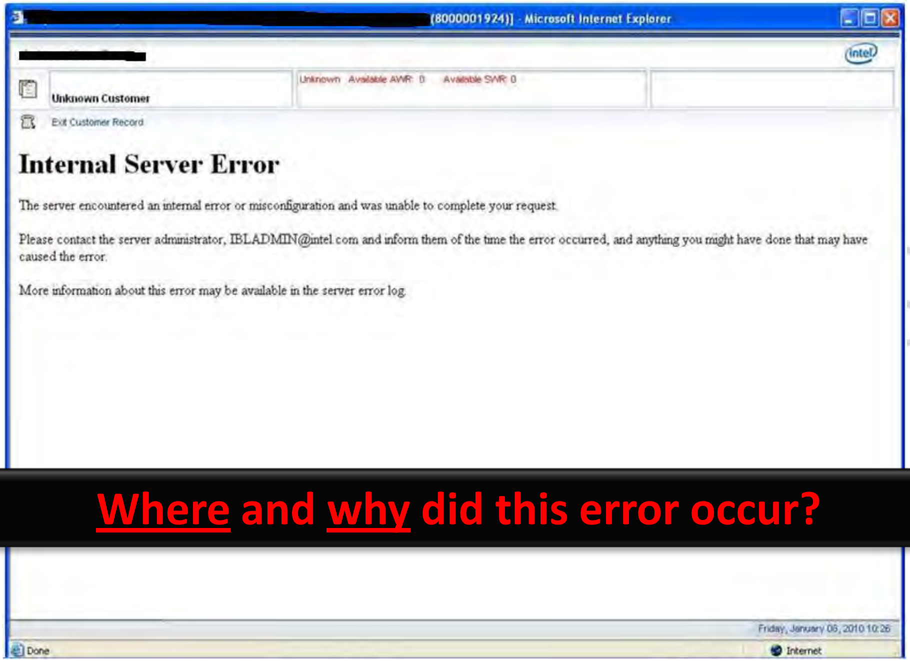
- Problem Statement
- Methodology
- Testing Details
- Analysis & Inferences

Summary

SHARKFEST '10

Problem Statement

Users were intermittently receiving an "**Internal Server Error**" when accessing an external facing website



[redacted] (8000001924)] - Microsoft Internet Explorer

[redacted]

Unknown Customer

Unknown Available AWR: 0 Available SWR: 0

Exit Customer Record

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, IBLADMIN@intel.com and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

Friday, January 08, 2010 10:26

Where and why did this error occur?

Methodology

Understand the application flow through the DMZ infrastructure

Capture interesting traffic

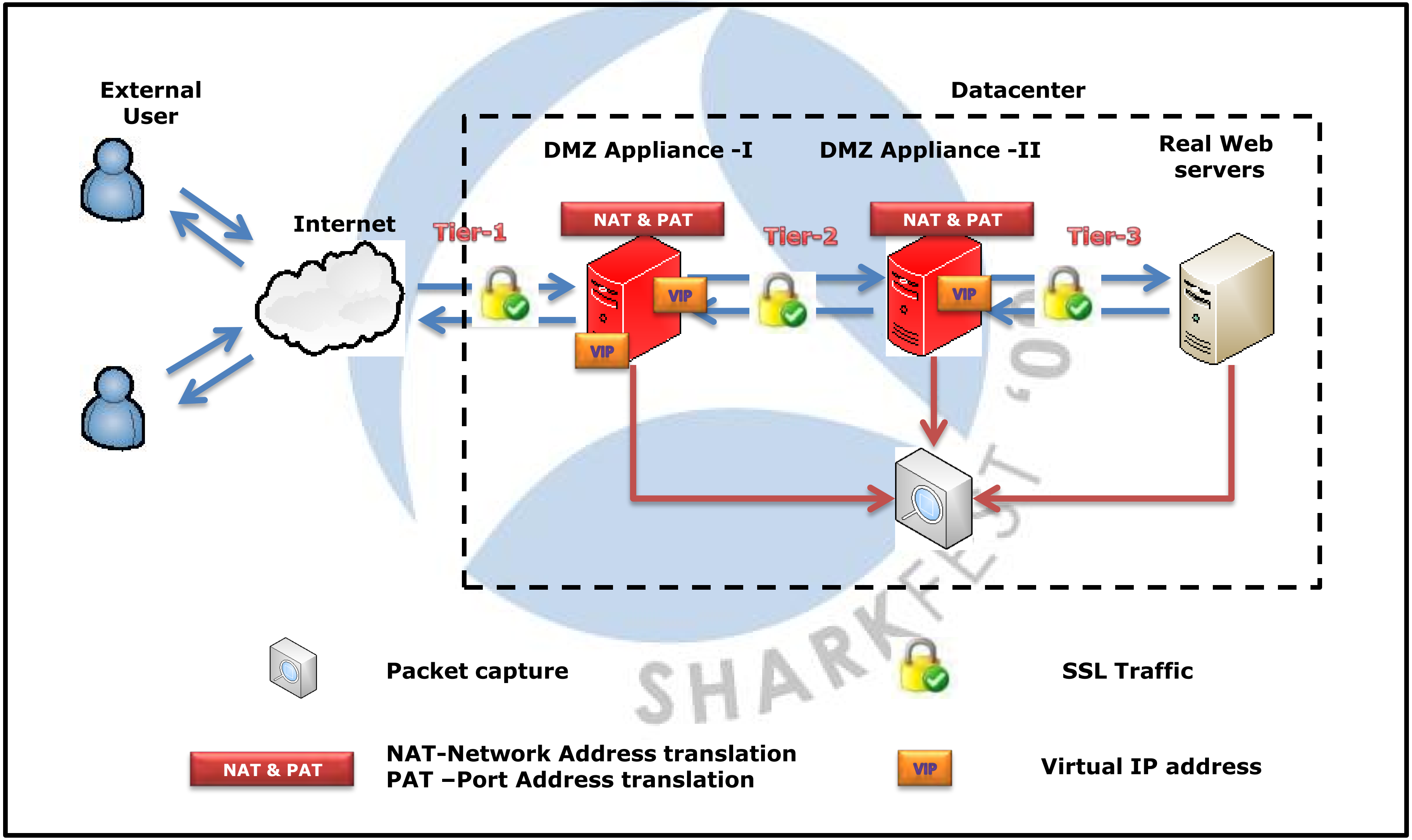
Filter based on the time of the error event

Decrypt the traffic to provide visibility

Analyze the traffic

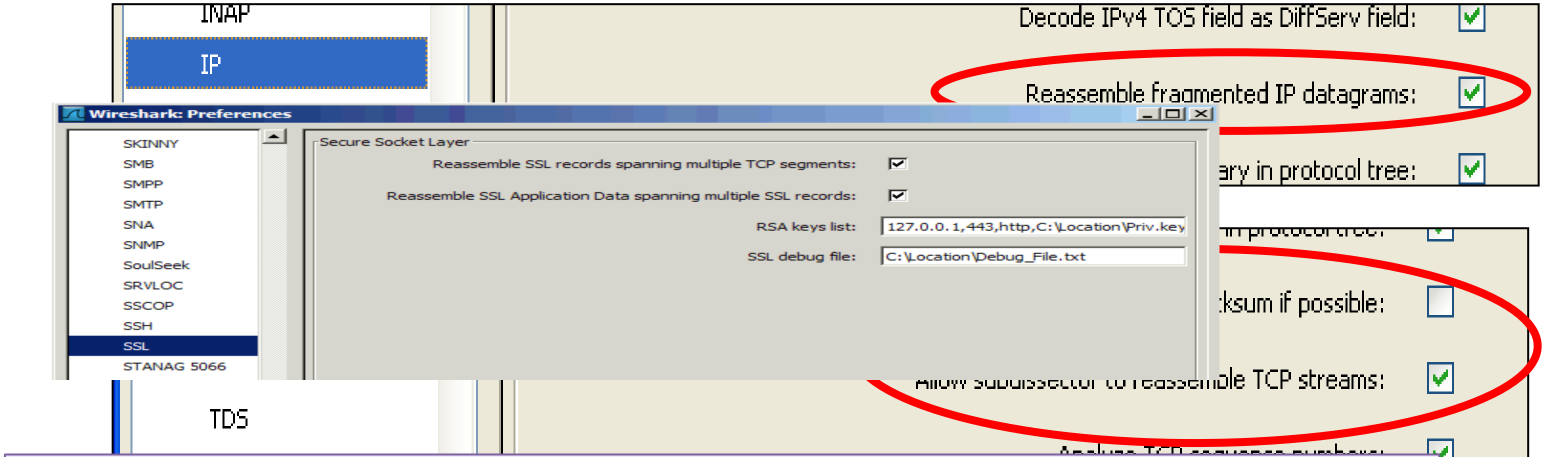
Correlate the findings to identify the root cause

Understand the Flow -
Capture the Interesting Traffic



SHARKFEST '0

Decrypt the Traffic



Decode IPv4 TOS field as DiffServ field: ☑

Reassemble fragmented IP datagrams: ☑

ary in protocol tree: ☑

ksum if possible: □

Allow subdissector to reassemble TCP streams: ☑

Secure Socket Layer

Reassemble SSL records spanning multiple TCP segments: ☑

Reassemble SSL Application Data spanning multiple SSL records: ☑

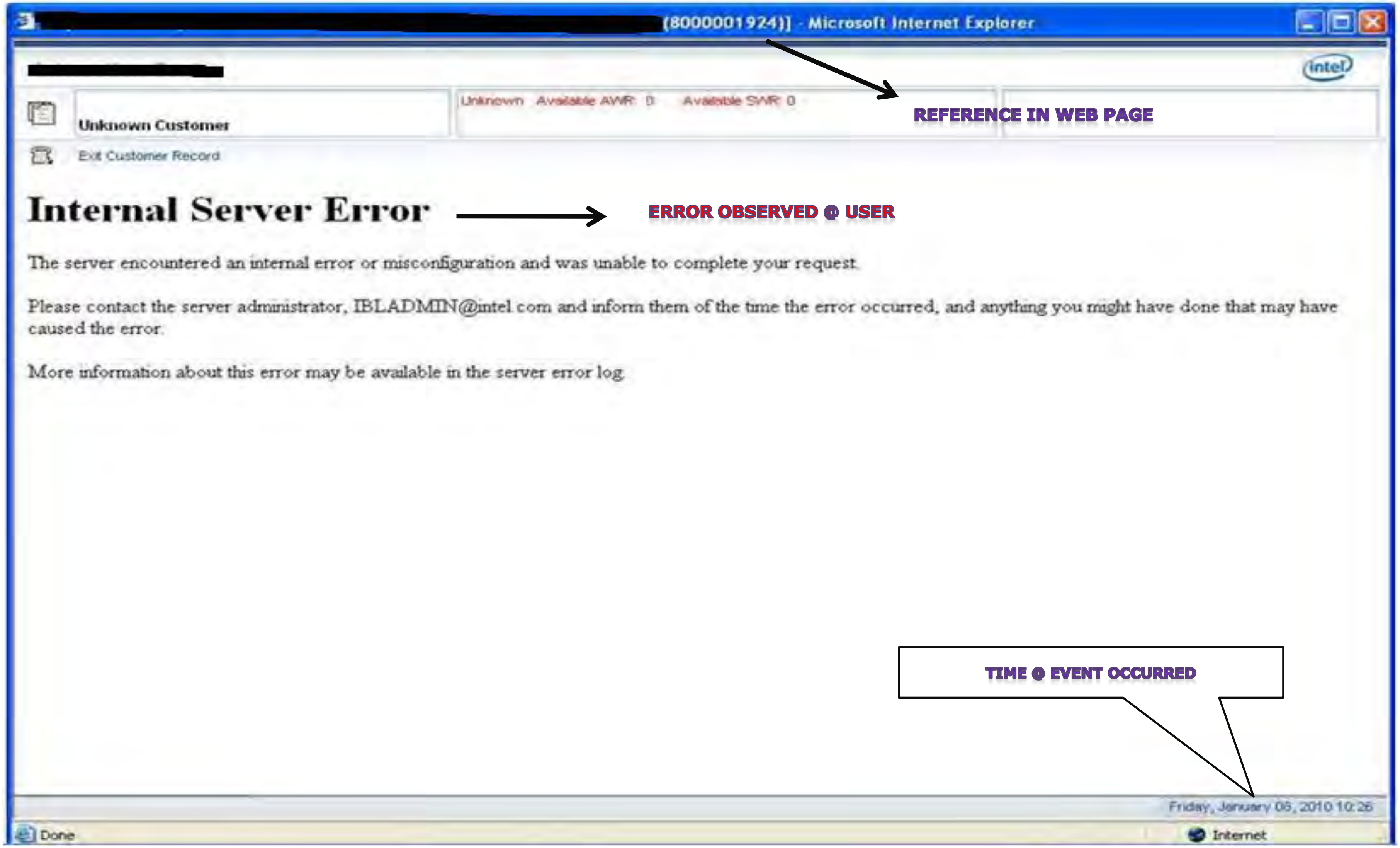
RSA keys list: 127.0.0.1,443,http,C:\Location\Priv.key

SSL debug file: C:\Location\Debug_File.txt

Where:
IP: is the IP Address of the server / appliance with the private key
Port: is usually 443 for SSL/TLS or destination port seen in the trace file
Protocol :is usually HTTP
Key File_Name: is the location and file name of the private key

For more info please refer "SSL Troubleshooting with Wireshark and Tshark" By Sake Blok in SHARKFEST '09

DMZ Tier-1 Observations



[redacted] (8000001924)] - Microsoft Internet Explorer

[redacted]

Unknown Customer

Unknown Available AWR: 0 Available SWR: 0

Exit Customer Record

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, IBLADMIN@intel.com and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

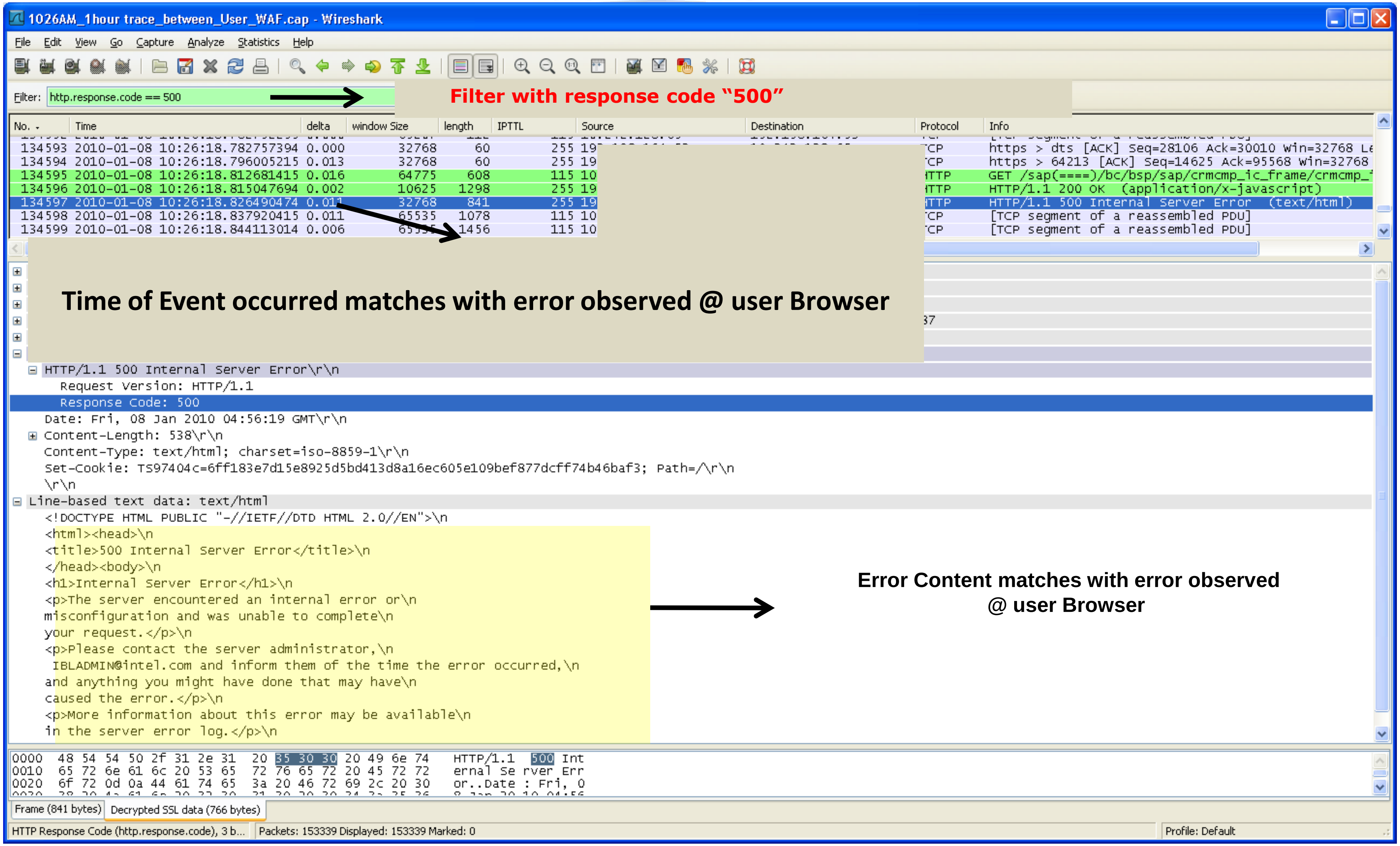
Friday, January 06, 2010 10:26

REFERENCE IN WEB PAGE

ERROR OBSERVED @ USER

TIME @ EVENT OCCURRED

DMZ Tier-1 Observations Cont..


1026AM_1hour trace_between_User_WAF.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: http.response.code == 500

Filter with response code "500"

```
No. .  Time                           delta  window Size  length  IPTTL  Source  Destination  Protocol  Info
134593 2010-01-08 10:26:18.782757394 0.000       32768      60    255 19                      CP        https > dts [ACK] Seq=28106 Ack=30010 Win=32768 Le
134594 2010-01-08 10:26:18.796005215 0.013       32768      60    255 19                      CP        https > 64213 [ACK] Seq=14625 Ack=95568 Win=32768
134595 2010-01-08 10:26:18.812681415 0.016       64775     608    115 10                      HTTP      GET /sap(====)/bc/bsp/sap/crmcmp_ic_frame/crmcmp_
134596 2010-01-08 10:26:18.815047694 0.002       10625    1298    255 19                      HTTP      HTTP/1.1 200 OK  (application/x-javascript)
134597 2010-01-08 10:26:18.826490474 0.011       32768     841    255 19                      HTTP      HTTP/1.1 500 Internal Server Error  (text/html)
134598 2010-01-08 10:26:18.837920415 0.011       65535    1078    115 10                      CP        [TCP segment of a reassembled PDU]
134599 2010-01-08 10:26:18.844113014 0.006       65535    1456    115 10                      CP        [TCP segment of a reassembled PDU]
```

Time of Event occurred matches with error observed @ user Browser

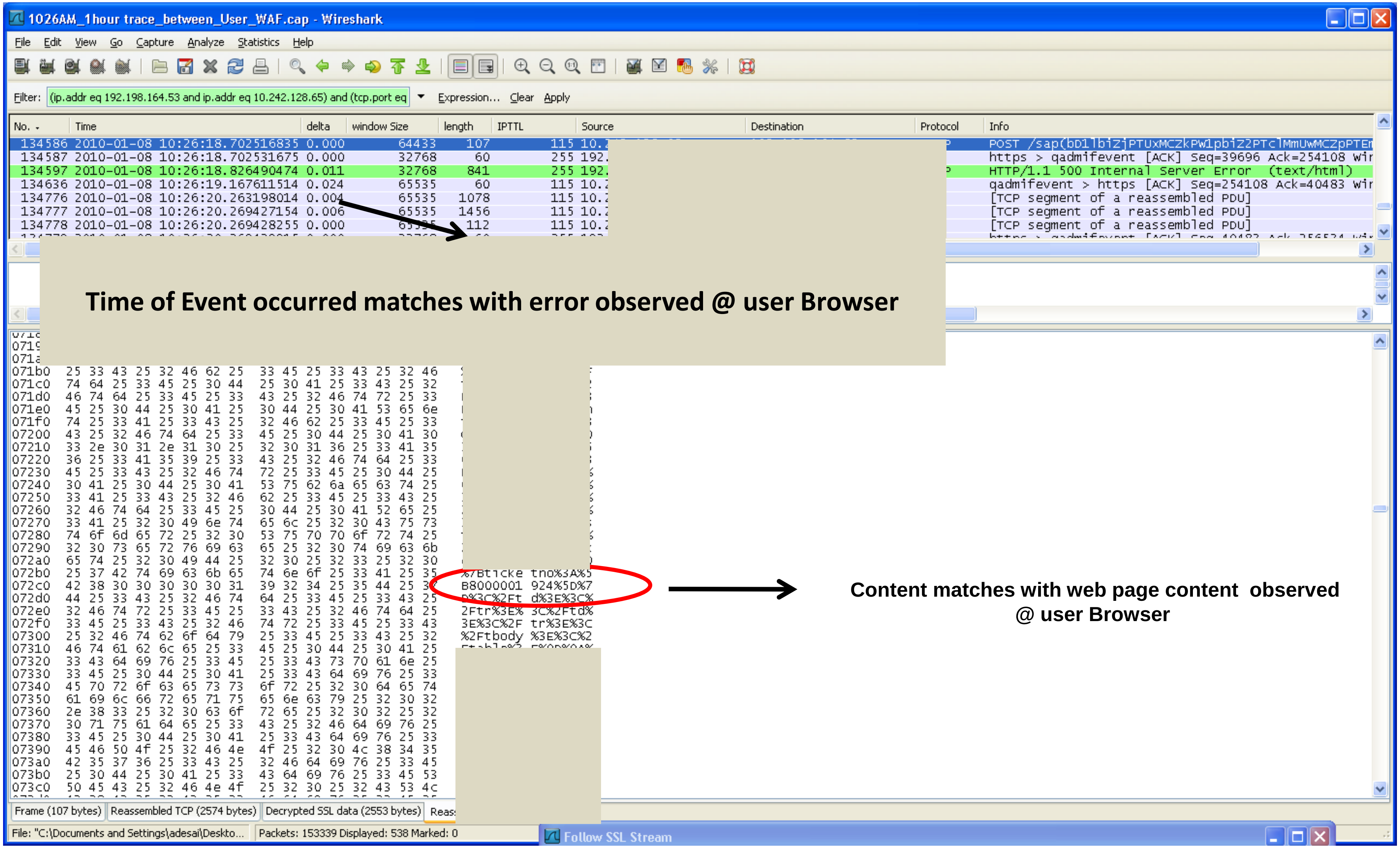
```
  HTTP/1.1 500 Internal Server Error\r\n
    Request Version: HTTP/1.1
    Response Code: 500
  Date: Fri, 08 Jan 2010 04:56:19 GMT\r\n
  Content-Length: 538\r\n
  Content-Type: text/html; charset=iso-8859-1\r\n
  Set-Cookie: TS97404c=6ff183e7d15e8925d5bd413d8a16ec605e109bef877dcff74b46baf3; Path=/\r\n
  \r\n
Line-based text data: text/html
  <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
  <html><head>\n
  <title>500 Internal Server Error</title>\n
  </head><body>\n
  <h1>Internal Server Error</h1>\n
  <p>The server encountered an internal error or\n
  misconfiguration and was unable to complete\n
  your request.</p>\n
  <p>Please contact the server administrator,\n
   IBLADMIN@intel.com and inform them of the time the error occurred,\n
  and anything you might have done that may have\n
  caused the error.</p>\n
  <p>More information about this error may be available\n
  in the server error log.</p>\n
```

Error Content matches with error observed @ user Browser

```
0000   48 54 54 50 2f 31 2e 31   20 35 30 30 20 49 6e 74    HTTP/1.1  500 Int
0010   65 72 6e 61 6c 20 53 65   72 76 65 72 20 45 72 72    ernal Se rver Err
0020   6f 72 0d 0a 44 61 74 65   3a 20 46 72 69 2c 20 30    or..Date : Fri, 0
```

Frame (841 bytes)
Decrypted SSL data (766 bytes)
HTTP Response Code (http.response.code), 3 b...
Packets: 153339 Displayed: 153339 Marked: 0
Profile: Default

DMZ Tier-1 Observations Cont..



1026AM_1hour trace_between_User_WAF.cap - Wireshark

Filter: (ip.addr eq 192.198.164.53 and ip.addr eq 10.242.128.65) and (tcp.port eq

```
No. -  Time                           delta  window Size  length  IPTTL  Source    Destination  Protocol  Info
134586 2010-01-08 10:26:18.702516835 0.000      64433      107     115 10.2 [redacted]           POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTc1MmUwMCZpPTEm
134587 2010-01-08 10:26:18.702531675 0.000      32768       60     255 192.                      https > qadmifevent [ACK] Seq=39696 Ack=254108 Wir
134597 2010-01-08 10:26:18.826490474 0.011      32768      841     255 192.                      HTTP/1.1 500 Internal Server Error  (text/html)
134636 2010-01-08 10:26:19.167611514 0.024      65535       60     115 10.2                      qadmifevent > https [ACK] Seq=254108 Ack=40483 Wir
134776 2010-01-08 10:26:20.263198014 0.004      65535     1078     115 10.2                      [TCP segment of a reassembled PDU]
134777 2010-01-08 10:26:20.269427154 0.006      65535     1456     115 10.2                      [TCP segment of a reassembled PDU]
134778 2010-01-08 10:26:20.269428255 0.000      65535      112     115 10.2                      [TCP segment of a reassembled PDU]
```

Time of Event occurred matches with error observed @ user Browser

```
071b0  25 33 43 25 32 46 62 25  33 45 25 33 43 25 32 46   [redacted]
071c0  74 64 25 33 45 25 30 44  25 30 41 25 33 43 25 32
071d0  46 74 64 25 33 45 25 33  43 25 32 46 74 72 25 33
071e0  45 25 30 44 25 30 41 25  30 44 25 30 41 53 65 6e
071f0  74 25 33 41 25 33 43 25  32 46 62 25 33 45 25 33
07200  43 25 32 46 74 64 25 33  45 25 30 44 25 30 41 30
07210  33 2e 30 31 2e 31 30 25  32 30 31 36 25 33 41 35
07220  36 25 33 41 35 39 25 33  43 25 32 46 74 64 25 33
07230  45 25 33 43 25 32 46 74  72 25 33 45 25 30 44 25
07240  30 41 25 30 44 25 30 41  53 75 62 6a 65 63 74 25
07250  33 41 25 33 43 25 32 46  62 25 33 45 25 33 43 25
07260  32 46 74 64 25 33 45 25  30 44 25 30 41 52 65 25
07270  33 41 25 32 30 49 6e 74  65 6c 25 32 30 43 75 73
07280  74 6f 6d 65 72 25 32 30  53 75 70 70 6f 72 74 25
07290  32 30 73 65 72 76 69 63  65 25 32 30 74 69 63 6b
072a0  65 74 25 32 30 49 44 25  32 30 25 32 33 25 32 30
072b0  25 37 42 74 69 63 6b 65  74 6e 6f 25 33 41 25 35   %7Bticke tno%3A%5
072c0  42 38 30 30 30 30 30 31  39 32 34 25 35 44 25 37   B8000001 924%5D%7
072d0  44 25 33 43 25 32 46 74  64 25 33 45 25 33 43 25   D%3C%2Ft d%3E%3C%
072e0  32 46 74 72 25 33 45 25  33 43 25 32 46 74 64 25   2Ftr%3E% 3C%2Ftd%
072f0  33 45 25 33 43 25 32 46  74 72 25 33 45 25 33 43   3E%3C%2F tr%3E%3C
07300  25 32 46 74 62 6f 64 79  25 33 45 25 33 43 25 32   %2Ftbody %3E%3C%2
07310  46 74 61 62 6c 65 25 33  45 25 30 44 25 30 41 25   [redacted]
07320  33 43 64 69 76 25 33 45  25 33 43 73 70 61 6e 25
07330  33 45 25 30 44 25 30 41  25 33 43 64 69 76 25 33
07340  45 70 72 6f 63 65 73 73  6f 72 25 32 30 64 65 74
07350  61 69 6c 66 72 65 71 75  65 6e 63 79 25 32 30 32
07360  2e 38 33 25 32 30 63 6f  72 65 25 32 30 32 25 32
07370  30 71 75 61 64 65 25 33  43 25 32 46 64 69 76 25
07380  33 45 25 30 44 25 30 41  25 33 43 64 69 76 25 33
07390  45 46 50 4f 25 32 46 4e  4f 25 32 30 4c 38 34 35
073a0  42 35 37 36 25 33 43 25  32 46 64 69 76 25 33 45
073b0  25 30 44 25 30 41 25 33  43 64 69 76 25 33 45 53
073c0  50 45 43 25 32 46 4e 4f  25 32 30 25 32 43 53 4c
```

Frame (107 bytes) | Reassembled TCP (2574 bytes) | Decrypted SSL data (2553 bytes) | Reas

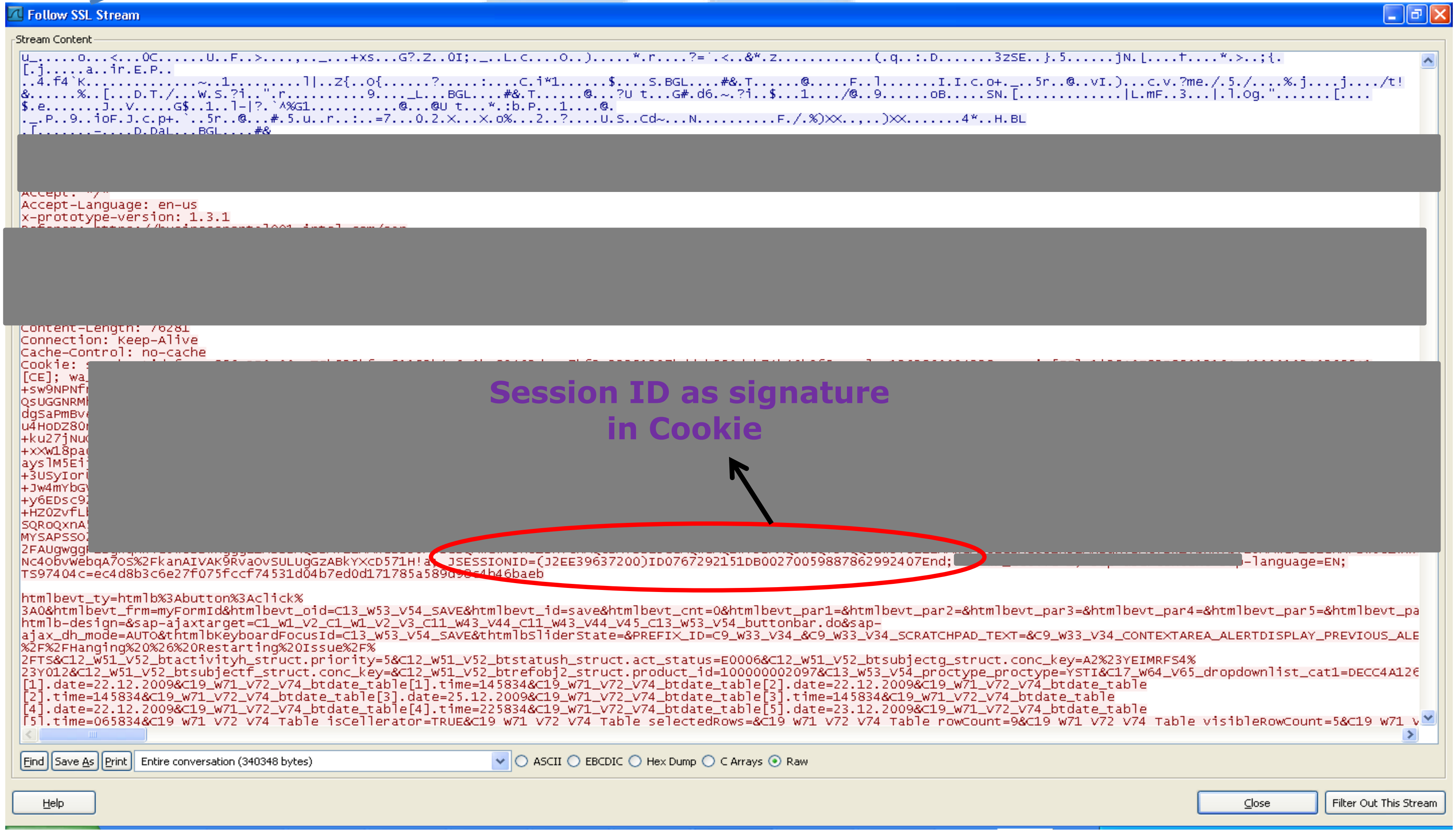
File: "C:\Documents and Settings\adesai\Deskto... | Packets: 153339 Displayed: 538 Marked: 0

Follow SSL Stream

Content matches with web page content observed @ user Browser

DMZ Tier-1 Observations Cont..

Using Follow SSL stream to filter the interested SSL flow



```
u_.....o...<...0C......U..F..>....,.._...+xs...G?.Z..0I;._..L.c....O..).....*.r....?=`.<..&*.z............(.q..:.D.......3zSE..}.5......jN.[....†....*.>..;{.
[.j.....a..ir.E.P..
..4.f4`K..............~..1.........]|..z{..o{......?.....:....C.i*1......$....S.BGL....#&.T......@.....F..].......I.I.c.o+._..5r..@..vI.)...c.v.?me./.5./....%.j....j..../t!
&......%..[...D.T./...W.S.?i..".r..........9...._L...BGL....#&.T......@...?U t...G#.d6.~.?i..$...1..../@..9......oB.....SN.[.............|L.mF..3...|.].og."........[....
$.e.......J..V.....G$..1..]-|?.`^%G1..........@...@U t...*.:b.P...1....@.
._.P..9..ioF.J.c.p+.`..5r..@...#.5.u..r..:..=7...0.2.X...X.o%...2..?....U.S..Cd~...N..........F./.%)XX..,..)XX.......4*..H.BL
```

[redacted]

```
Accept-Language: en-us
x-prototype-version: 1.3.1
```

[redacted]

```
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:
[CE]; wa
+sw9NPNf
QsUGGNRM
dgSaPmBv
u4HoDZ80
+ku27jNu
+xXw18pa
aysIM5Ei
+3USyIor
+Jw4mYbG
+y6EDsc9
+HZOZvfL
SQRoQxnA
MYSAPSSO
2FAUgwgg
```

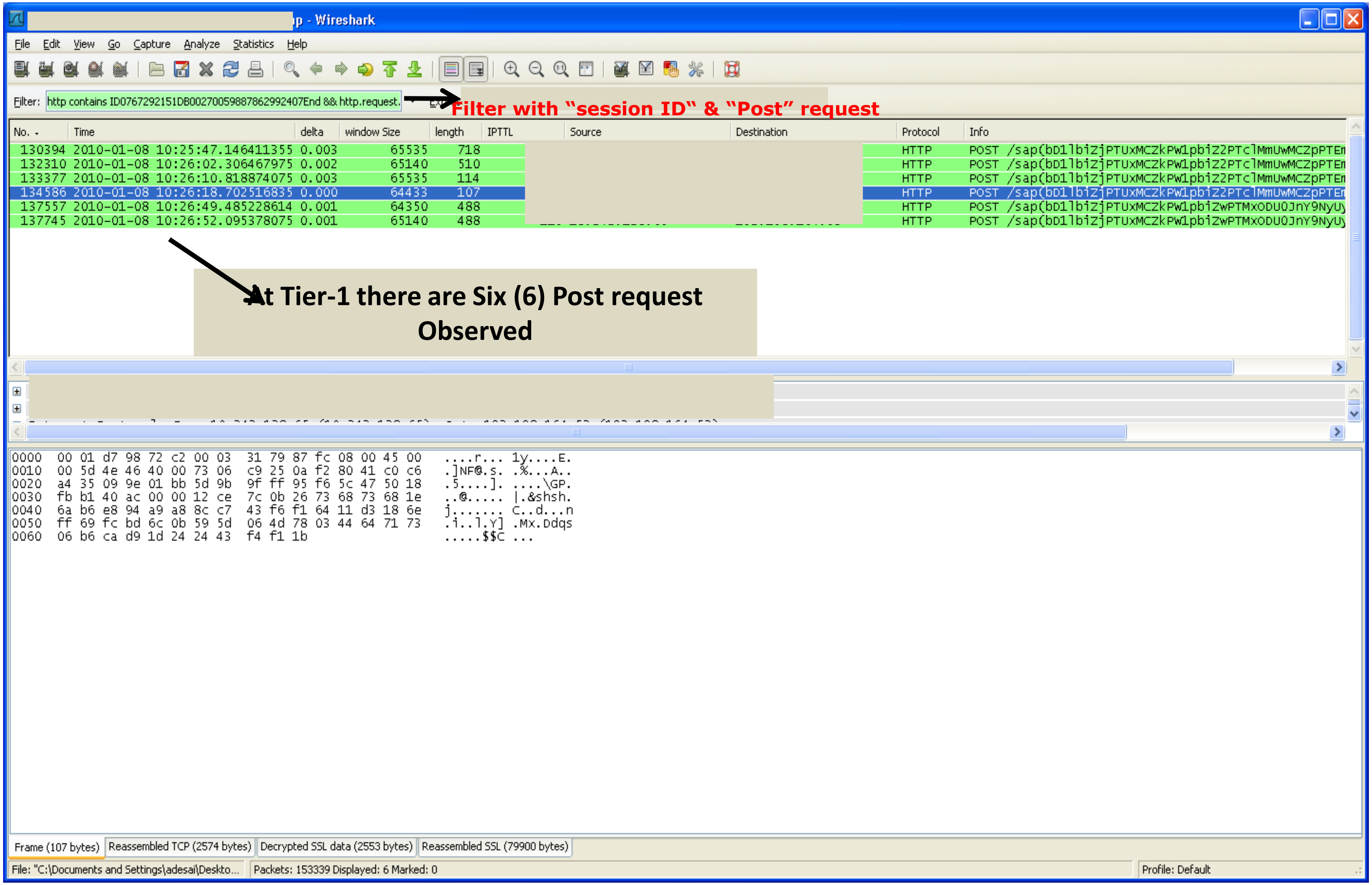
[redacted]

```
Nc4ObvwebqA7OS%2FkanAIVAK9RvaOvSULUgGZABkYXcD571H!a  JSESSIONID=(J2EE39637200)ID0767292151DB00270059887862992407End; [redacted] -language=EN;
TS97404c=ec4d8b3c6e27f075fccf74531d04b7ed0d171785a589d9[illegible]4b46baeb

htmlbevt_ty=htmlb%3Abutton%3Aclick%
3A0&htmlbevt_frm=myFormId&htmlbevt_oid=C13_W53_V54_SAVE&htmlbevt_id=save&htmlbevt_cnt=0&htmlbevt_par1=&htmlbevt_par2=&htmlbevt_par3=&htmlbevt_par4=&htmlbevt_par5=&htmlbevt_pa
htmlb-design=&sap-ajaxtarget=C1_W1_V2_C1_W1_V2_V3_C11_W43_V44_C11_W43_V44_V45_C13_W53_V54_buttonbar.do&sap-
ajax_dh_mode=AUTO&thtmlbKeyboardFocusId=C13_W53_V54_SAVE&thtmlbSliderState=&PREFIX_ID=C9_W33_V34_&C9_W33_V34_SCRATCHPAD_TEXT=&C9_W33_V34_CONTEXTAREA_ALERTDISPLAY_PREVIOUS_ALE
%2F%2FHanging%20%26%20Restarting%20Issue%2F%
2FTS&C12_W51_V52_btactivityh_struct.priority=5&C12_W51_V52_btstatush_struct.act_status=E0006&C12_W51_V52_btsubjectg_struct.conc_key=A2%23YEIMRFS4%
23Y012&C12_W51_V52_btsubjectf_struct.conc_key=&C12_W51_V52_btrefobj2_struct.product_id=10000002097&C13_W53_V54_proctype_proctype=YSTI&C17_W64_V65_dropdownlist_cat1=DECC4A126
[1].date=22.12.2009&C19_W71_V72_V74_btdate_table[1].time=145834&C19_W71_V72_V74_btdate_table[2].date=22.12.2009&C19_W71_V72_V74_btdate_table
[2].time=145834&C19_W71_V72_V74_btdate_table[3].date=25.12.2009&C19_W71_V72_V74_btdate_table[3].time=145834&C19_W71_V72_V74_btdate_table
[4].date=22.12.2009&C19_W71_V72_V74_btdate_table[4].time=225834&C19_W71_V72_V74_btdate_table[5].date=23.12.2009&C19_W71_V72_V74_btdate_table
[5].time=065834&C19 W71 V72 V74 Table isCellerator=TRUE&C19 W71 V72 V74 Table selectedRows=&C19 W71 V72 V74 Table rowCount=9&C19 W71 V72 V74 Table visibleRowCount=5&C19 W71 V
```

Session ID as signature in Cookie

DMZ Tier-1 Observations Cont..



Filter: http contains ID0767292151DB00270059887862992407End && http.request.

Filter with "session ID" & "Post" request

No.	Time	delta	window Size	length	IPTTL	Source	Destination	Protocol	Info
130394	2010-01-08 10:25:47.146411355	0.003	65535	718	[redacted]	[redacted]	[redacted]	HTTP	POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEm
132310	2010-01-08 10:26:02.306467975	0.002	65140	510	[redacted]	[redacted]	[redacted]	HTTP	POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEm
133377	2010-01-08 10:26:10.818874075	0.003	65535	114	[redacted]	[redacted]	[redacted]	HTTP	POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEm
134586	2010-01-08 10:26:18.702516835	0.000	64433	107	[redacted]	[redacted]	[redacted]	HTTP	POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEm
137557	2010-01-08 10:26:49.485228614	0.001	64350	488	[redacted]	[redacted]	[redacted]	HTTP	POST /sap(bD1lbizjPTUxMCZkPW1pbiZwPTMxODU0JnY9NyUy
137745	2010-01-08 10:26:52.095378075	0.001	65140	488	[redacted]	[redacted]	[redacted]	HTTP	POST /sap(bD1lbizjPTUxMCZkPW1pbiZwPTMxODU0JnY9NyUy

At Tier-1 there are Six (6) Post request Observed

[redacted]

```
0000   00 01 d7 98 72 c2 00 03  31 79 87 fc 08 00 45 00   ....r... 1y....E.
0010   00 5d 4e 46 40 00 73 06  c9 25 0a f2 80 41 c0 c6   .]NF@.s. .%...A..
0020   a4 35 09 9e 01 bb 5d 9b  9f ff 95 f6 5c 47 50 18   .5....]. ....\GP.
0030   fb b1 40 ac 00 00 12 ce  7c 0b 26 73 68 73 68 1e   ..@..... |.&shsh.
0040   6a b6 e8 94 a9 a8 8c c7  43 f6 f1 64 11 d3 18 6e   j....... C..d...n
0050   ff 69 fc bd 6c 0b 59 5d  06 4d 78 03 44 64 71 73   .i..l.Y] .Mx.Ddqs
0060   06 b6 ca d9 1d 24 24 43  f4 f1 1b                  .....$$C ...
```

Frame (107 bytes) | Reassembled TCP (2574 bytes) | Decrypted SSL data (2553 bytes) | Reassembled SSL (79900 bytes)

File: "C:\Documents and Settings\adesai\Deskto... | Packets: 153339 Displayed: 6 Marked: 0 | Profile: Default

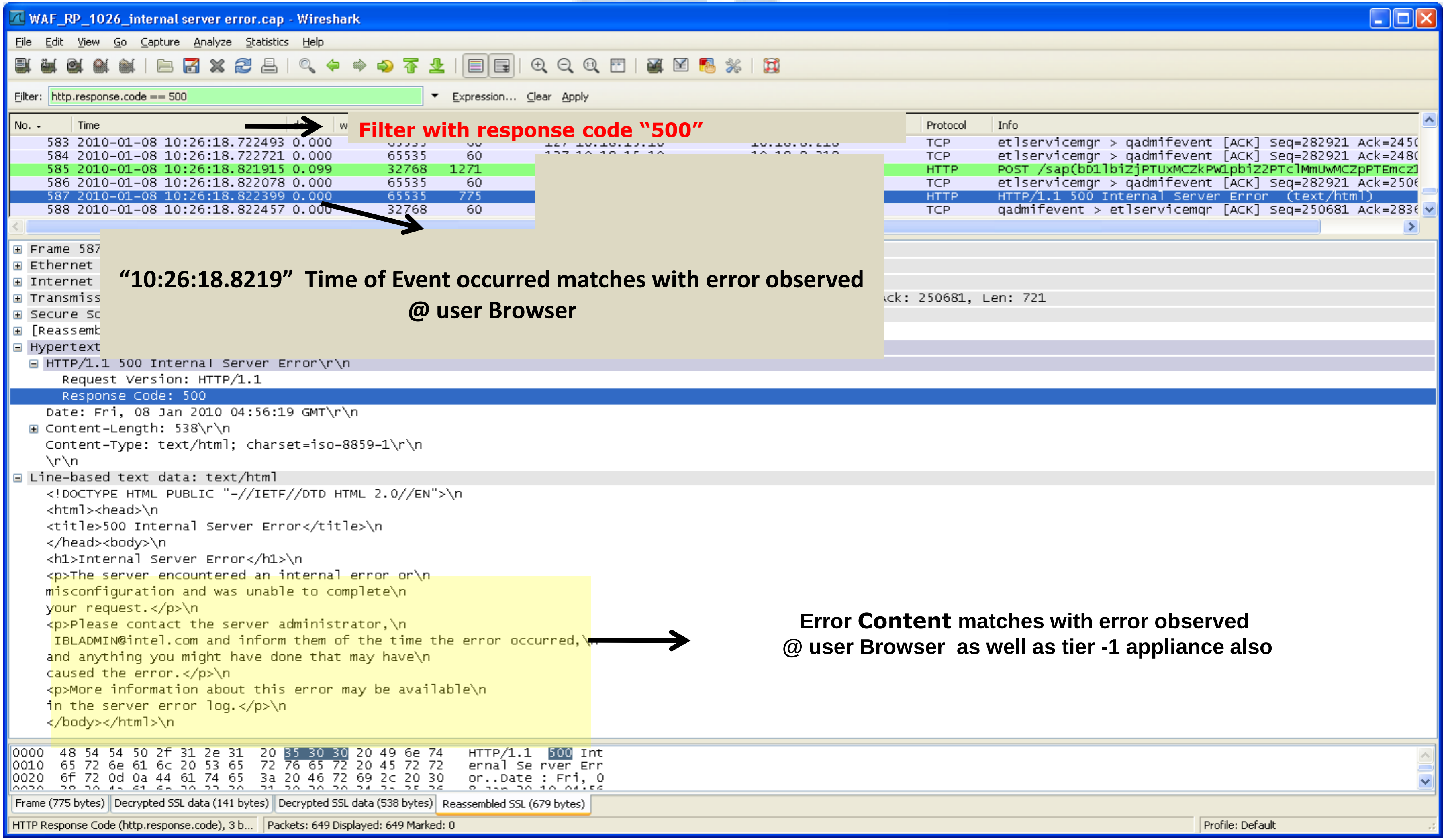
Signature Identified

Signature identified from Tier-1 to track to next level of DMZ Appliances

- Time of event occurred : **10:26:18:8264 AM**
- Cookie info – session ID: **ID0767292151DB00270059887862992407End**
- Number of Post request in interesting SSL stream: **6**
- Content info in web page : “**800001924**”

SHARKFEST '10

DMZ Tier-2 Observations


WAF_RP_1026_internal server error.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
Profile: Default

Filter: http.response.code == 500

Filter with response code “500”

```
No. .  Time                                                              Protocol  Info
   583 2010-01-08 10:26:18.722493 0.000                                  TCP       etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=245(
   584 2010-01-08 10:26:18.722721 0.000   65535     60                   TCP       etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=248(
   585 2010-01-08 10:26:18.821915 0.099   32768   1271                   HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
   586 2010-01-08 10:26:18.822078 0.000   65535     60                   TCP       etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=250(
   587 2010-01-08 10:26:18.822399 0.000   65535    775                   HTTP      HTTP/1.1 500 Internal Server Error  (text/html)
   588 2010-01-08 10:26:18.822457 0.000   32768     60                   TCP       qadmifevent > etlservicemgr [ACK] Seq=250681 Ack=283(
```

“10:26:18.8219” Time of Event occurred matches with error observed @ user Browser

```
⊞ Frame 587
⊞ Ethernet
⊞ Internet
⊞ Transmiss                                                         ck: 250681, Len: 721
⊞ Secure So
⊞ [Reassemb
⊟ Hypertext
  ⊟ HTTP/1.1 500 Internal Server Error\r\n
      Request Version: HTTP/1.1
      Response Code: 500
    Date: Fri, 08 Jan 2010 04:56:19 GMT\r\n
  ⊞ Content-Length: 538\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
⊟ Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>500 Internal Server Error</title>\n
    </head><body>\n
    <h1>Internal Server Error</h1>\n
    <p>The server encountered an internal error or\n
    misconfiguration and was unable to complete\n
    your request.</p>\n
    <p>Please contact the server administrator,\n
     IBLADMIN@intel.com and inform them of the time the error occurred,\n
    and anything you might have done that may have\n
    caused the error.</p>\n
    <p>More information about this error may be available\n
    in the server error log.</p>\n
    </body></html>\n
```

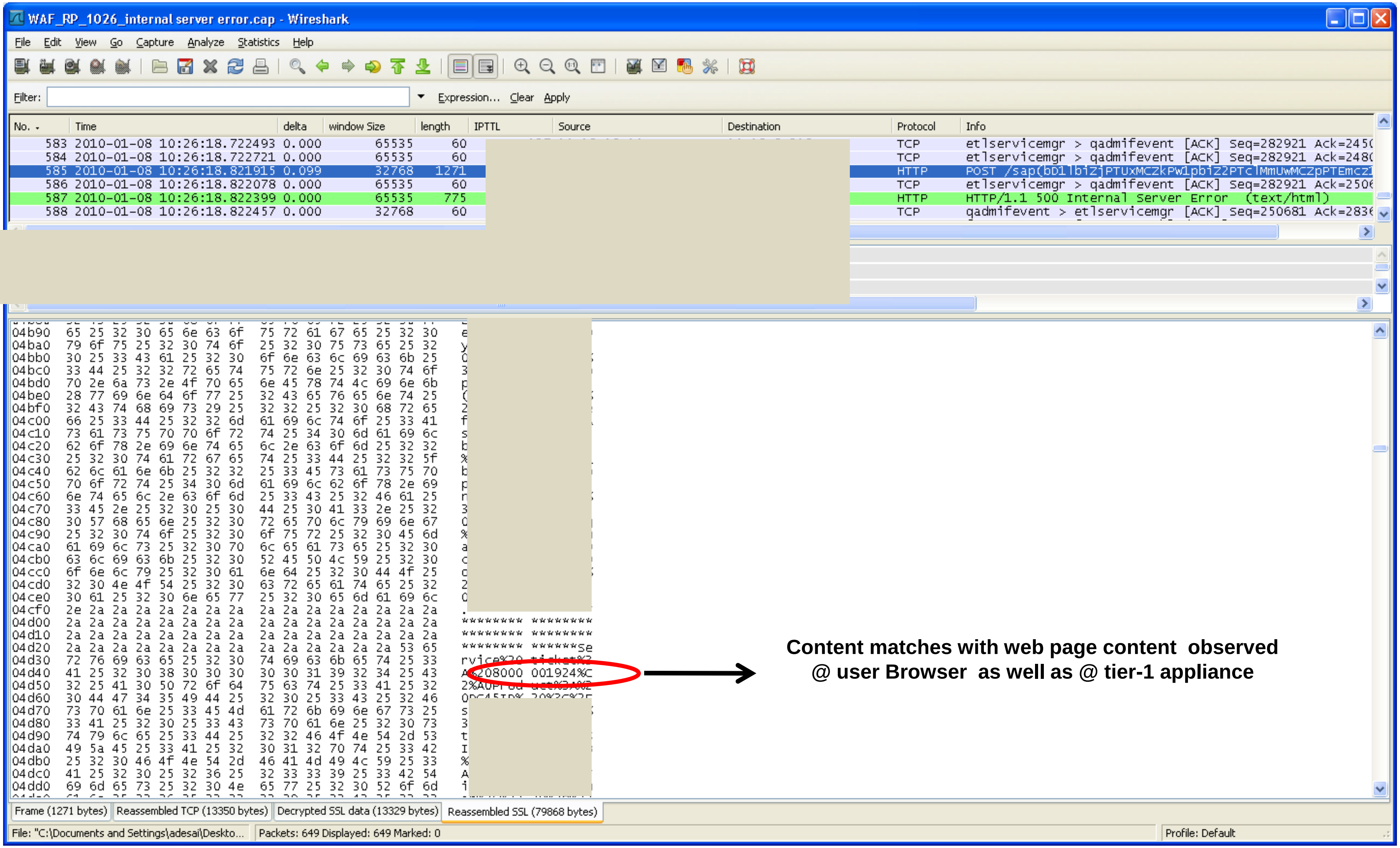
Error Content matches with error observed @ user Browser as well as tier -1 appliance also

```
0000  48 54 54 50 2f 31 2e 31  20 35 30 30 20 49 6e 74   HTTP/1.1  500 Int
0010  65 72 6e 61 6c 20 53 65  72 76 65 72 20 45 72 72   ernal Se rver Err
0020  6f 72 0d 0a 44 61 74 65  3a 20 46 72 69 2c 20 30   or..Date : Fri, 0
```

Frame (775 bytes) | Decrypted SSL data (141 bytes) | Decrypted SSL data (538 bytes) | Reassembled SSL (679 bytes)

HTTP Response Code (http.response.code), 3 b... | Packets: 649 Displayed: 649 Marked: 0

DMZ Tier-2 Observations, Cont..



WAF_RP_1026_internal server error.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time                       delta  window Size  length  IPTTL  Source  Destination  Protocol  Info
  583 2010-01-08 10:26:18.722493 0.000        65535      60   [redacted]                 TCP       etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=245(
  584 2010-01-08 10:26:18.722721 0.000        65535      60                              TCP       etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=248(
  585 2010-01-08 10:26:18.821915 0.099        32768    1271                              HTTP      POST /sap(bD1lbiZjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
  586 2010-01-08 10:26:18.822078 0.000        65535      60                              TCP       etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=250(
  587 2010-01-08 10:26:18.822399 0.000        65535     775                              HTTP      HTTP/1.1 500 Internal Server Error  (text/html)
  588 2010-01-08 10:26:18.822457 0.000        32768      60                              TCP       qadmifevent > etlservicemgr [ACK] Seq=250681 Ack=283(
```

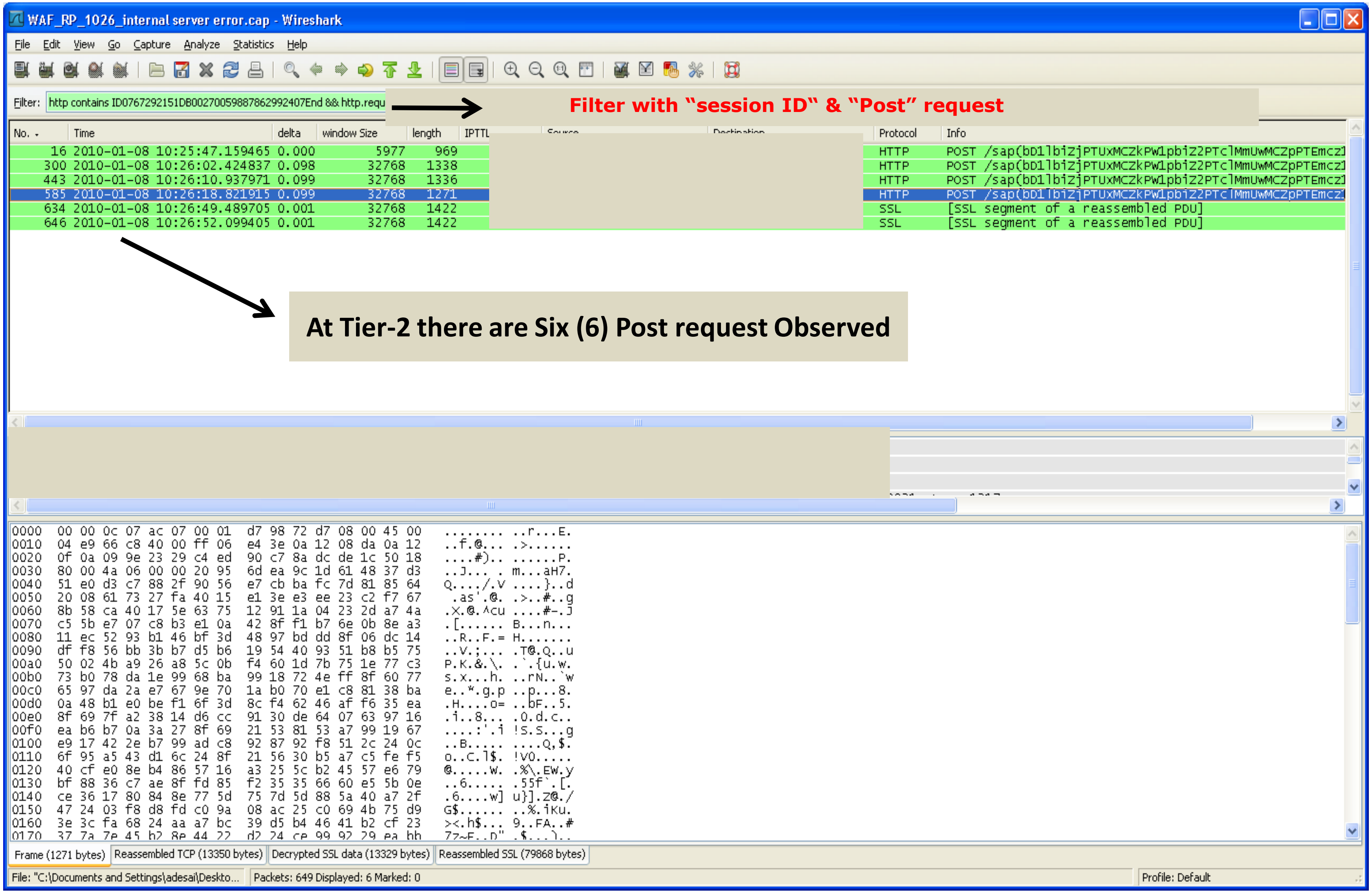
[redacted]

```
04b90  65 25 32 30 65 6e 63 6f  75 72 61 67 65 25 32 30   e[redacted]
04ba0  79 6f 75 25 32 30 74 6f  25 32 30 75 73 65 25 32   y
04bb0  30 25 33 43 61 25 32 30  6f 6e 63 6c 69 63 6b 25   0
04bc0  33 44 25 32 32 72 65 74  75 72 6e 25 32 30 74 6f   3
04bd0  70 2e 6a 73 2e 4f 70 65  6e 45 78 74 4c 69 6e 6b   p
04be0  28 77 69 6e 64 6f 77 25  32 43 65 76 65 6e 74 25   (
04bf0  32 43 74 68 69 73 29 25  32 32 25 32 30 68 72 65   2
04c00  66 25 33 44 25 32 32 6d  61 69 6c 74 6f 25 33 41   f
04c10  73 61 73 75 70 70 6f 72  74 25 34 30 6d 61 69 6c   s
04c20  62 6f 78 2e 69 6e 74 65  6c 2e 63 6f 6d 25 32 32   b
04c30  25 32 30 74 61 72 67 65  74 25 33 44 25 32 32 5f   %
04c40  62 6c 61 6e 6b 25 32 32  25 33 45 73 61 73 75 70   b
04c50  70 6f 72 74 25 34 30 6d  61 69 6c 62 6f 78 2e 69   p
04c60  6e 74 65 6c 2e 63 6f 6d  25 33 43 25 32 46 61 25   n
04c70  33 45 2e 25 32 30 25 30  44 25 30 41 33 2e 25 32   3
04c80  30 57 68 65 6e 25 32 30  72 65 70 6c 79 69 6e 67   0
04c90  25 32 30 74 6f 25 32 30  6f 75 72 25 32 30 45 6d   %
04ca0  61 69 6c 73 25 32 30 70  6c 65 61 73 65 25 32 30   a
04cb0  63 6c 69 63 6b 25 32 30  52 45 50 4c 59 25 32 30   c
04cc0  6f 6e 6c 79 25 32 30 61  6e 64 25 32 30 44 4f 25   o
04cd0  32 30 4e 4f 54 25 32 30  63 72 65 61 74 65 25 32   2
04ce0  30 61 25 32 30 6e 65 77  25 32 30 65 6d 61 69 6c   0
04cf0  2e 2a 2a 2a 2a 2a 2a 2a  2a 2a 2a 2a 2a 2a 2a 2a   .
04d00  2a 2a 2a 2a 2a 2a 2a 2a  2a 2a 2a 2a 2a 2a 2a 2a   ******** ********
04d10  2a 2a 2a 2a 2a 2a 2a 2a  2a 2a 2a 2a 2a 2a 2a 2a   ******** ********
04d20  2a 2a 2a 2a 2a 2a 2a 2a  2a 2a 2a 2a 2a 2a 53 65   ******** ******Se
04d30  72 76 69 63 65 25 32 30  74 69 63 6b 65 74 25 33   rvice%20 ticket%3
04d40  41 25 32 30 38 30 30 30  30 30 31 39 32 34 25 43   A%208000 001924%C
04d50  32 25 41 30 50 72 6f 64  75 63 74 25 33 41 25 32   2%A0Prod uct%3A%2
04d60  30 44 47 34 35 49 44 25  32 30 25 33 43 25 32 46   0DG45ID% 20%3C%2F
04d70  73 70 61 6e 25 33 45 4d  61 72 6b 69 6e 67 73 25   s[redacted]
04d80  33 41 25 32 30 25 33 43  73 70 61 6e 25 32 30 73   3
04d90  74 79 6c 65 25 33 44 25  32 32 46 4f 4e 54 2d 53   t
04da0  49 5a 45 25 33 41 25 32  30 31 32 70 74 25 33 42   I
04db0  25 32 30 46 4f 4e 54 2d  46 41 4d 49 4c 59 25 33   %
04dc0  41 25 32 30 25 32 36 25  32 33 33 39 25 33 42 54   A
04dd0  69 6d 65 73 25 32 30 4e  65 77 25 32 30 52 6f 6d   i
```

Frame (1271 bytes)
Reassembled TCP (13350 bytes)
Decrypted SSL data (13329 bytes)
Reassembled SSL (79868 bytes)
File: "C:\Documents and Settings\adesai\Deskto...
Packets: 649 Displayed: 649 Marked: 0
Profile: Default

Content matches with web page content observed @ user Browser as well as @ tier-1 appliance

DMZ Tier-2 Observations, Cont..



Filter: http contains ID0767292151DB00270059887862992407End && http.requ

Filter with "session ID" & "Post" request

```
No.  Time                        delta  window Size  length  IPTTL  Source      Destination  Protocol  Info
 16  2010-01-08 10:25:47.159465  0.000        5977     969          [redacted]  [redacted]   HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
300  2010-01-08 10:26:02.424837  0.098       32768    1338          [redacted]  [redacted]   HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
443  2010-01-08 10:26:10.937971  0.099       32768    1336          [redacted]  [redacted]   HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
585  2010-01-08 10:26:18.821915  0.099       32768    1271          [redacted]  [redacted]   HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
634  2010-01-08 10:26:49.489705  0.001       32768    1422          [redacted]  [redacted]   SSL       [SSL segment of a reassembled PDU]
646  2010-01-08 10:26:52.099405  0.001       32768    1422          [redacted]  [redacted]   SSL       [SSL segment of a reassembled PDU]
```

At Tier-2 there are Six (6) Post request Observed

[redacted]

```
0000  00 00 0c 07 ac 07 00 01  d7 98 72 d7 08 00 45 00   ........ ..r...E.
0010  04 e9 66 c8 40 00 ff 06  e4 3e 0a 12 08 da 0a 12   ..f.@... .>......
0020  0f 0a 09 9e 23 29 c4 ed  90 c7 8a dc de 1c 50 18   ....#).. ......P.
0030  80 00 4a 06 00 00 20 95  6d ea 9c 1d 61 48 37 d3   ..J... . m...aH7.
0040  51 e0 d3 c7 88 2f 90 56  e7 cb ba fc 7d 81 85 64   Q..../.V ....}..d
0050  20 08 61 73 27 fa 40 15  e1 3e e3 ee 23 c2 f7 67    .as'.@. .>..#..g
0060  8b 58 ca 40 17 5e 63 75  12 91 1a 04 23 2d a7 4a   .X.@.^cu ....#-.J
0070  c5 5b e7 07 c8 b3 e1 0a  42 8f f1 b7 6e 0b 8e a3   .[...... B...n...
0080  11 ec 52 93 b1 46 bf 3d  48 97 bd dd 8f 06 dc 14   ..R..F.= H.......
0090  df f8 56 bb 3b b7 d5 b6  19 54 40 93 51 b8 b5 75   ..V.;... .T@.Q..u
00a0  50 02 4b a9 26 a8 5c 0b  f4 60 1d 7b 75 1e 77 c3   P.K.&.\. .`.{u.w.
00b0  73 b0 78 da 1e 99 68 ba  99 18 72 4e ff 8f 60 77   s.x...h. ..rN..`w
00c0  65 97 da 2a e7 67 9e 70  1a b0 70 e1 c8 81 38 ba   e..*.g.p ..p...8.
00d0  0a 48 b1 e0 be f1 6f 3d  8c f4 62 46 af f6 35 ea   .H....o= ..bF..5.
00e0  8f 69 7f a2 38 14 d6 cc  91 30 de 64 07 63 97 16   .i..8... .0.d.c..
00f0  ea b6 b7 0a 3a 27 8f 69  21 53 81 53 a7 99 19 67   ....:'.i !S.S...g
0100  e9 17 42 2e b7 99 ad c8  92 87 92 f8 51 2c 24 0c   ..B..... ....Q,$.
0110  6f 95 a5 43 d1 6c 24 8f  21 56 30 b5 a7 c5 fe f5   o..C.l$. !V0.....
0120  40 cf e0 8e b4 86 57 16  a3 25 5c b2 45 57 e6 79   @.....W. .%\.EW.y
0130  bf 88 36 c7 ae 8f fd 85  f2 35 35 66 60 e5 5b 0e   ..6..... .55f`.[.
0140  ce 36 17 80 84 8e 77 5d  75 7d 5d 88 5a 40 a7 2f   .6....w] u}].Z@./
0150  47 24 03 f8 d8 fd c0 9a  08 ac 25 c0 69 4b 75 d9   G$...... ..%.iKu.
0160  3e 3c fa 68 24 aa a7 bc  39 d5 b4 46 41 b2 cf 23   ><.h$... 9..FA..#
0170  37 7a 7e 45 b2 8e 44 22  d2 24 ce 99 92 29 ea bb   7z~E..D" .$...)..
```

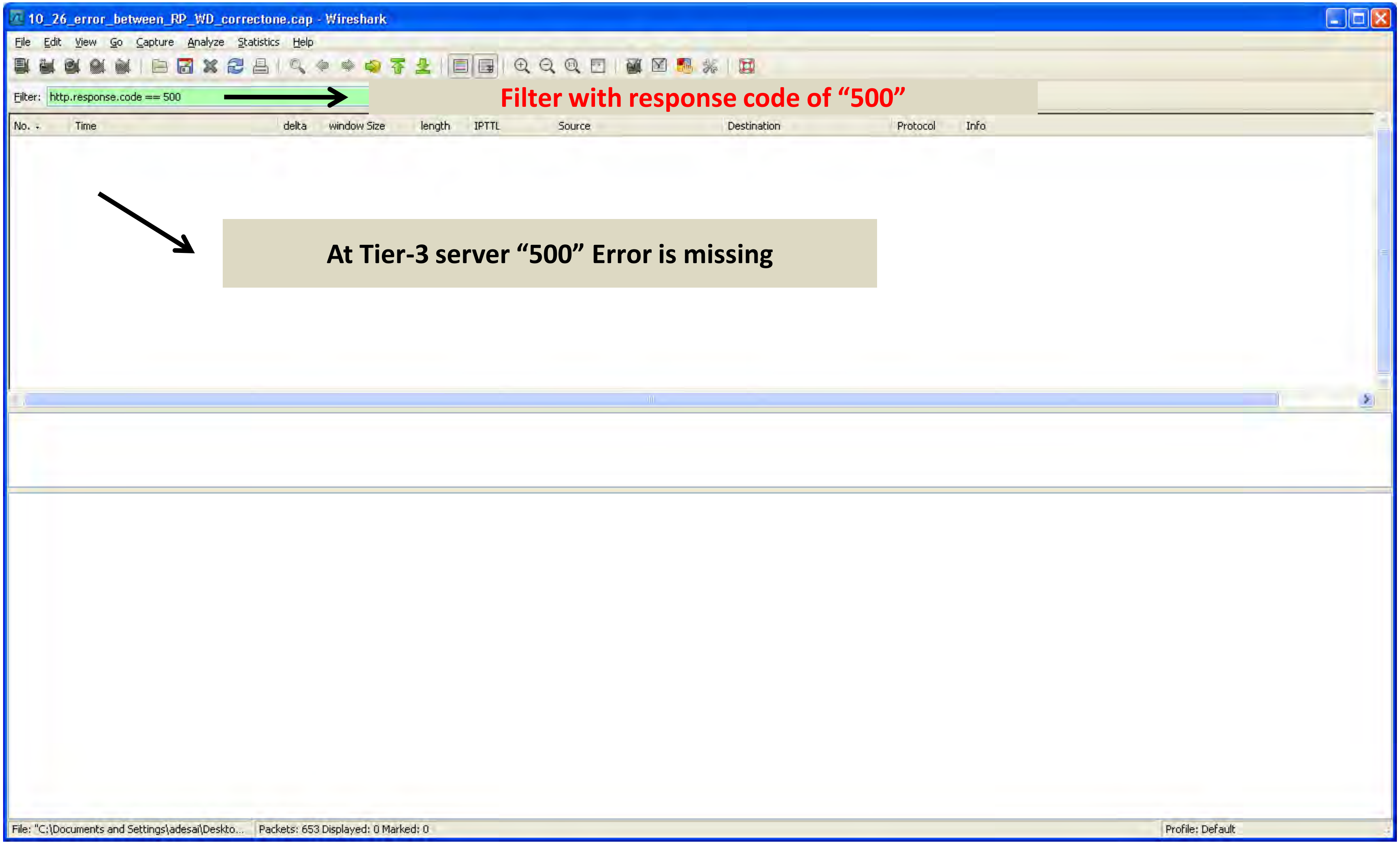
Frame (1271 bytes)
Reassembled TCP (13350 bytes)
Decrypted SSL data (13329 bytes)
Reassembled SSL (79868 bytes)

File: "C:\Documents and Settings\adesai\Deskto...

Packets: 649 Displayed: 6 Marked: 0

Profile: Default

DMZ Tier-3 Observations



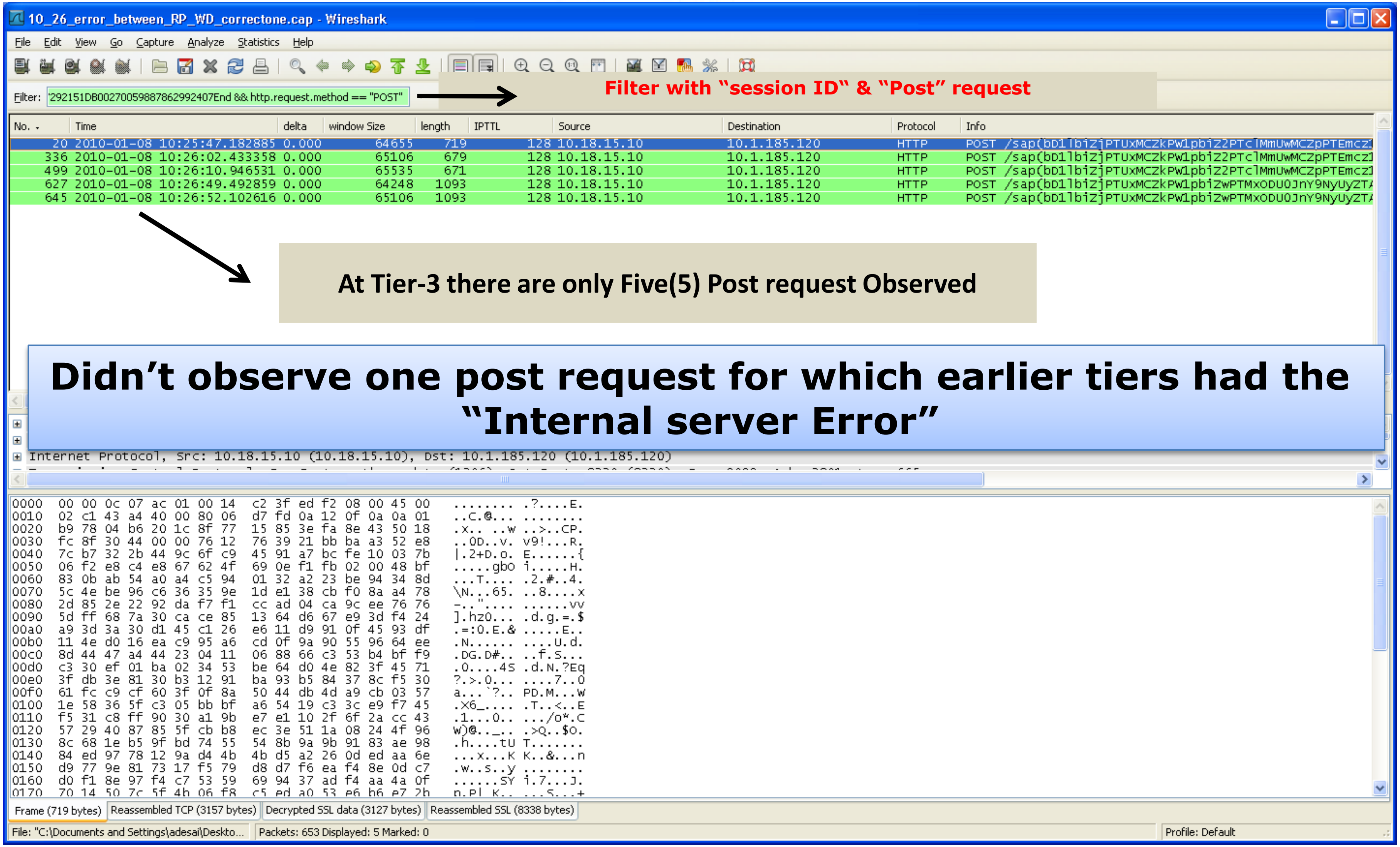
10_26_error_between_RP_WD_correctone.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: http.response.code == 500
No. Time delta window Size length IPTTL Source Destination Protocol Info

Filter with response code of “500”

At Tier-3 server “500” Error is missing

File: "C:\Documents and Settings\adesai\Deskto... Packets: 653 Displayed: 0 Marked: 0 Profile: Default

DMZ Tier-3 Observations, Cont..



10_26_error_between_RP_WD_correctone.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help

Filter: '292151DB0027005988 7862992407End && http.request.method == "POST"

Filter with "session ID" & "Post" request

```
No. .  Time                         delta  window Size  length  IPTTL  Source       Destination   Protocol  Info
    20 2010-01-08 10:25:47.182885  0.000       64655     719     128  10.18.15.10  10.1.185.120  HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
   336 2010-01-08 10:26:02.433358  0.000       65106     679     128  10.18.15.10  10.1.185.120  HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
   499 2010-01-08 10:26:10.946531  0.000       65535     671     128  10.18.15.10  10.1.185.120  HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZ2PTclMmUwMCZpPTEmcz1
   627 2010-01-08 10:26:49.492859  0.000       64248    1093     128  10.18.15.10  10.1.185.120  HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZwPTMxODU0JnY9NyUyZTA
   645 2010-01-08 10:26:52.102616  0.000       65106    1093     128  10.18.15.10  10.1.185.120  HTTP      POST /sap(bD1lbizjPTUxMCZkPW1pbiZwPTMxODU0JnY9NyUyZTA
```

At Tier-3 there are only Five(5) Post request Observed

Didn't observe one post request for which earlier tiers had the "Internal server Error"

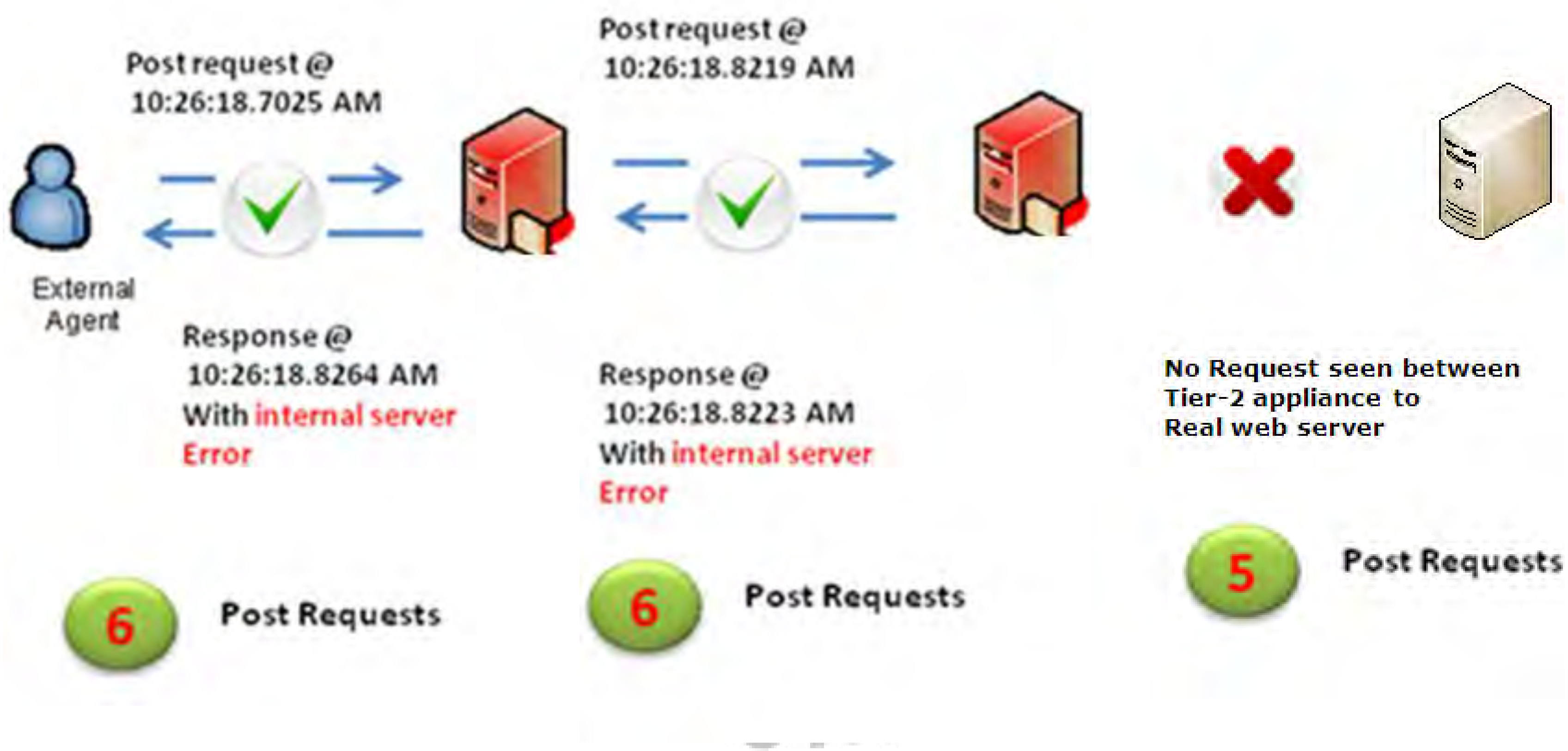
```
Internet Protocol, Src: 10.18.15.10 (10.18.15.10), Dst: 10.1.185.120 (10.1.185.120)
```

```
0000   00 00 0c 07 ac 01 00 14  c2 3f ed f2 08 00 45 00   ........ .?....E.
0010   02 c1 43 a4 40 00 80 06  d7 fd 0a 12 0f 0a 0a 01   ..C.@... ........
0020   b9 78 04 b6 20 1c 8f 77  15 85 3e fa 8e 43 50 18   .x.. ..w ..>..CP.
0030   fc 8f 30 44 00 00 76 12  76 39 21 bb ba a3 52 e8   ..0D..v. v9!...R.
0040   7c b7 32 2b 44 9c 6f c9  45 91 a7 bc fe 10 03 7b   |.2+D.o. E......{
0050   06 f2 e8 c4 e8 67 62 4f  69 0e f1 fb 02 00 48 bf   .....gbO i.....H.
0060   83 0b ab 54 a0 a4 c5 94  01 32 a2 23 be 94 34 8d   ...T.... .2.#..4.
0070   5c 4e be 96 c6 36 35 9e  1d e1 38 cb f0 8a a4 78   \N...65. ..8....x
0080   2d 85 2e 22 92 da f7 f1  cc ad 04 ca 9c ee 76 76   -..".... ......vv
0090   5d ff 68 7a 30 ca ce 85  13 64 d6 67 e9 3d f4 24   ].hz0... .d.g.=.$
00a0   a9 3d 3a 30 d1 45 c1 26  e6 11 d9 91 0f 45 93 df   .=:0.E.& .....E..
00b0   11 4e d0 16 ea c9 95 a6  cd 0f 9a 90 55 96 64 ee   .N...... ....U.d.
00c0   8d 44 47 a4 44 23 04 11  06 88 66 c3 53 b4 bf f9   .DG.D#.. ..f.S...
00d0   c3 30 ef 01 ba 02 34 53  be 64 d0 4e 82 3f 45 71   .0....4S .d.N.?Eq
00e0   3f db 3e 81 30 b3 12 91  ba 93 b5 84 37 8c f5 30   ?.>.0... ....7..0
00f0   61 fc c9 cf 60 3f 0f 8a  50 44 db 4d a9 cb 03 57   a...`?.. PD.M...W
0100   1e 58 36 5f c3 05 bb bf  a6 54 19 c3 3c e9 f7 45   .X6_.... .T..<..E
0110   f5 31 c8 ff 90 30 a1 9b  e7 e1 10 2f 6f 2a cc 43   .1...0.. .../o*.C
0120   57 29 40 87 85 5f cb b8  ec 3e 51 1a 08 24 4f 96   W)@.._.. .>Q..$O.
0130   8c 68 1e b5 9f bd 74 55  54 8b 9a 9b 91 83 ae 98   .h....tU T.......
0140   84 ed 97 78 12 9a d4 4b  4b d5 a2 26 0d ed aa 6e   ...x...K K..&...n
0150   d9 77 9e 81 73 17 f5 79  d8 d7 f6 ea f4 8e 0d c7   .w..s..y ........
0160   d0 f1 8e 97 f4 c7 53 59  69 94 37 ad f4 aa 4a 0f   ......SY i.7...J.
0170   70 14 50 7c 5f 4b 06 f8  c5 ed a0 53 e6 b6 e7 2b   p.P|_K.. ...S...+
```

Frame (719 bytes)
Reassembled TCP (3157 bytes)
Decrypted SSL data (3127 bytes)
Reassembled SSL (8338 bytes)

File: "C:\Documents and Settings\adesai\Deskto... Packets: 653 Displayed: 5 Marked: 0 Profile: Default

Analysis Summary



Post request @
10:26:18.7025 AM

Post request @
10:26:18.8219 AM

External Agent

Response @
10:26:18.8264 AM
With internal server Error

Response @
10:26:18.8223 AM
With internal server Error

No Request seen between
Tier-2 appliance to
Real web server

6 Post Requests

6 Post Requests

5 Post Requests

Root Cause Identified

Tier-2 appliance was not forwarding to next tier (real server) and was dropping the request.

In response, it sent an “Internal Server Error” to the requestor

Solution

Escalated to vendor regarding observations:

- Vendor acknowledged this is a software "bug"
- Suggested upgrading to prevent this issue

After upgrading, issue no longer seen! ☺

Presentation Summary

Understand the application flow to help you capture interesting traffic

Pay attention to any data that could be used as a "signature" to correlate traces with user events

Wireshark's capabilities of decryption, filtering, follow SSL stream, and others will help your analysis

X-forwarding can provide info on IP address/host, but to get visibility of user task look above IP layer

Questions?