Open Source Network Security Monitoring With Sguil

David J. Bianco
Cybersecurity Analyst
Jefferson Lab
bianco@jlab.org

Table of Contents

Network Monitoring

- Most mid/large-sized organizations perform network monitoring
  - Intrusion Detection Systems (IDS)
  - Syslogs/Event Logs
  - NetFlow/SFlow
  - Other sources(?)
- Lots of information but no coherence
  - Hard to correlate into usable intelligence
  - Difficult to reassemble the puzzle
  - Research & analysis takes lots of analyst time

Network Security Monitoring

The collection, analysis and escalation of indications and warnings to detect and respond to intrusions.

NSM in a Nutshell

- NSM is a methodology, not a product
- An extension/evolution of traditional network monitoring
- Integrates different sources into a single view
  - Easier to understand
  - Speeds the research process

How to do NSM

- Collect as much information as practical
- Present it to the analyst in ways that make sense
- Don’t waste analyst time!

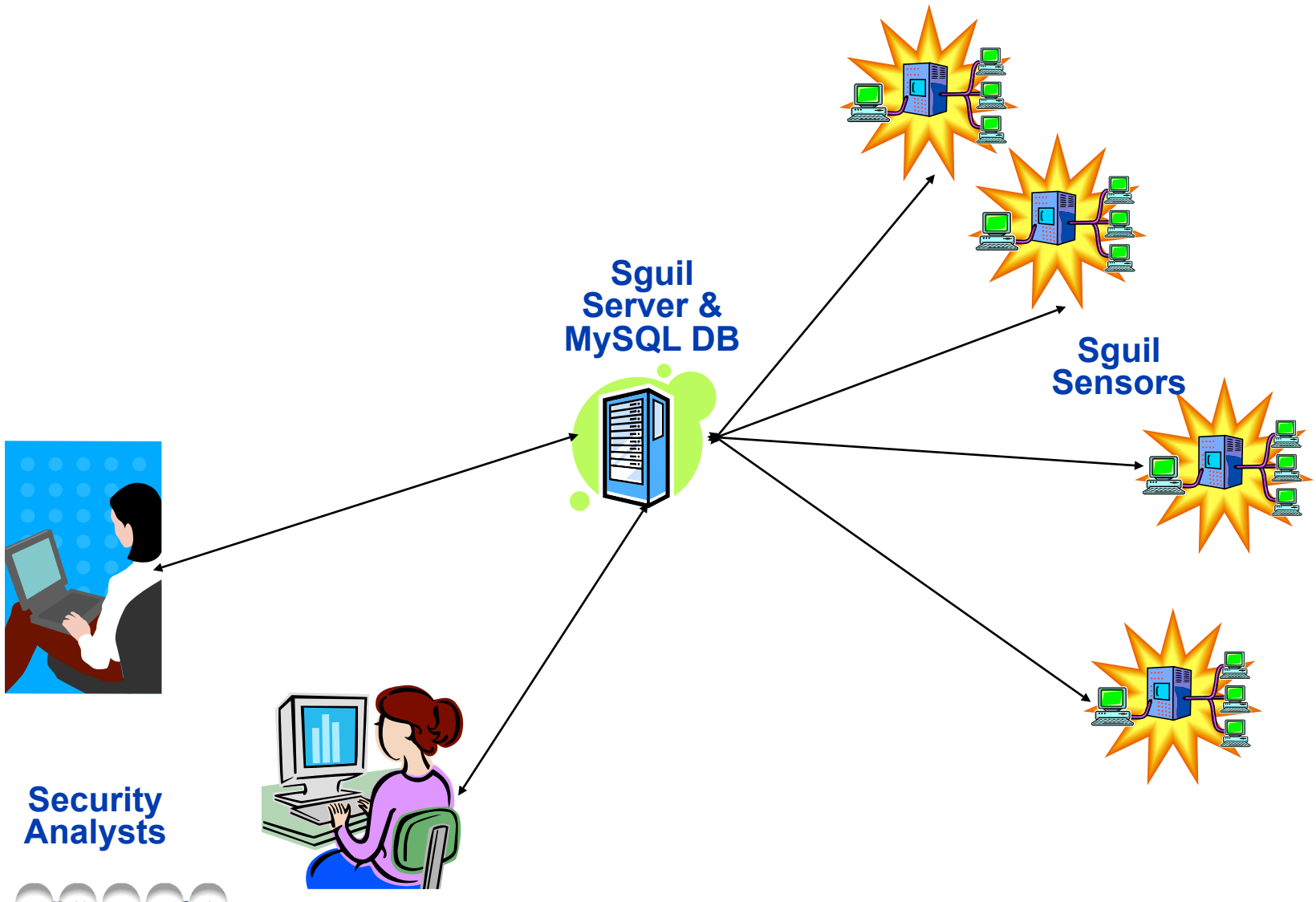
Types of NSM Data

- You need lots of data to do NSM
- Common types
  - IDS alerts
  - Network session data
  - Full packet content
  - DNS
  - WHOIS
  - Specialized/homebrew sources
    - Dial-up access logs
    - Application level audit logs
    - Anything else you might have handy

NSM With Sguil

- Open Source
- Developed by Bamm Vischer since 2002
- Name comes from “Snort GUI”
- Client
  - Tcl/Tk GUI for Unix/Linux/Windows
  - Also reported to work under OS X
- Server
  - Unix/Linux only
  - Tcl glue code around individual monitoring utilities

Sguil 3-Tiered Architecture



Sguil Sensor Components

- IDS (Snort)
  - Sourcefire VRT rules, Bleeding Snort and/or locally-developed rules
  - Recommend using Oinkmaster to manage rule updates
- Session information collection (SANCP)
  - Security Analyst Network Connection Profiler
  - Records who talks to whom, start & end times, number of bytes and packets transferred
  - Covers TCP, UDP, ICMP
- Full network packet capture (Snort)
  - Needs LOTS of disk space
  - Automatically manages available storage
  - Tunable to store as much or as little as you like
  - Data retention varies by traffic observed & size of storage area

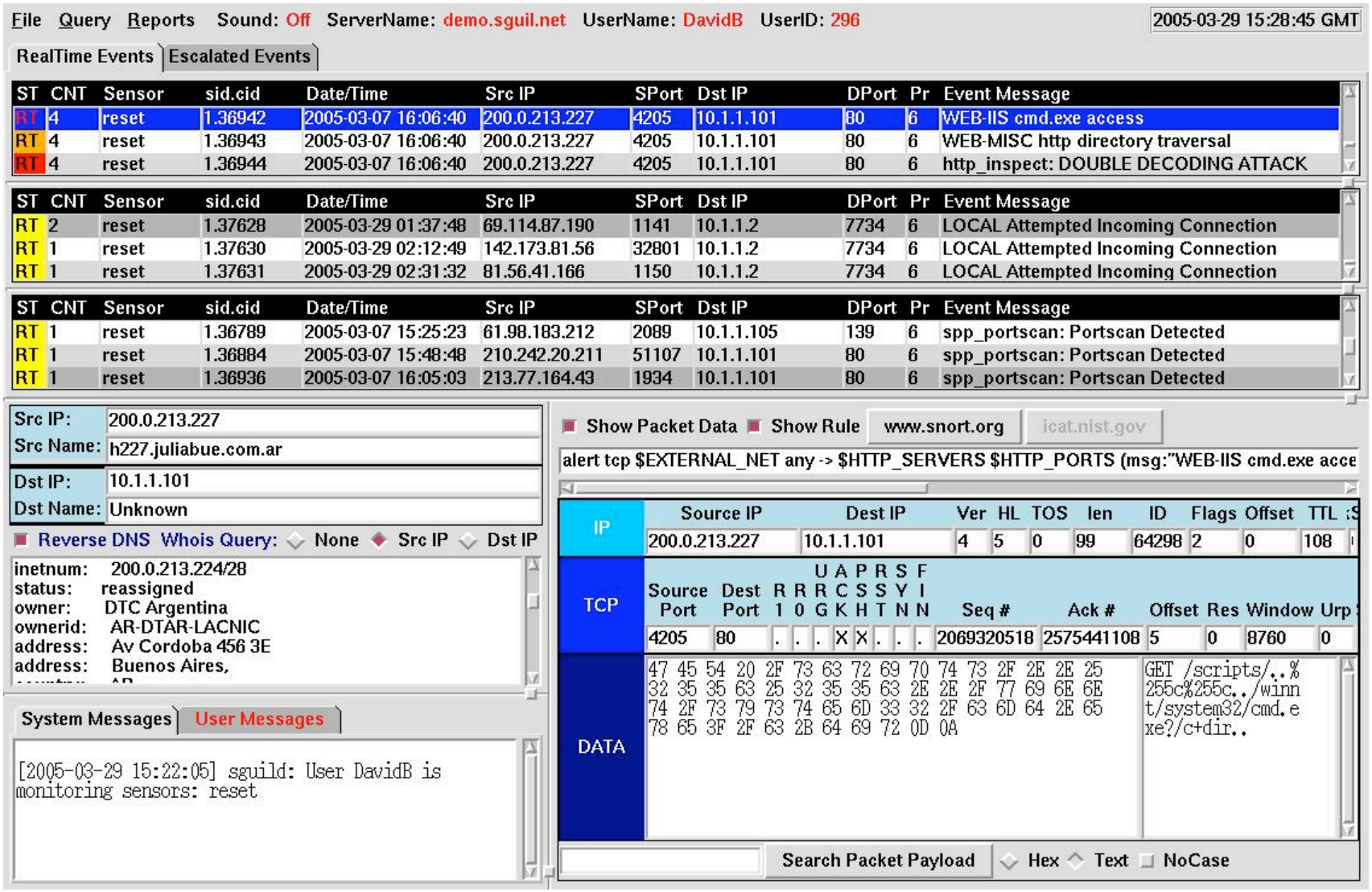
Sguil Server Components

- Sguil daemon (sguild)
  - Accepts connections from clients
  - Coordinates client requests with sensor data and MySQL DB
- MySQL DB
  - IDS alerts
  - Session information
  - Misc. related data
- SQL queries against network security data is a HUGE benefit
  - Greatly speeds up routine investigations
  - Easier to confirm/deny reports from external sources
  - Great for statistical anomaly detection and trend analysis
  - Allows us to capture metrics and generate reports

Data Flow

- IDS and session (SANCP) data
  - Collected on each sensor
  - Forwarded to the central server
    - Inserted into the database
    - IDS alerts may be sent via email/pager if necessary
  - Deleted from sensor
- Packet logs always stored on sensors
  - Server requests these when needed

Sguil Main Screen



Working With Sguil

- Analysts typically start with IDS alerts displayed on the console, then use the NSM data to research and make decisions
- Each alert must be dealt with. Analysts can:
  - Categorize the alert based on type of activity
  - Escalate the alert to a more senior analyst
- One of these two things must eventually happen!
  - Sguil is not an alert browser

Working With Sguil

- Once alerts are categorized, they disappear from the console
  - Still in the database until they expire
  - Available for reporting or further analysis at a later date
- Sguil provides full logging and audit trail of alert activity
  - Who took the action
  - When they took the action
  - Optional comments (why they took the action)

Working With Sguil

- Analysts don't have to start with alerts
- Scenario: Your upstream ISP has reported an IP address in your range that it suspects is "doing bad things", but you've noticed nothing in your IDS alerts.
- Response: Use the IP address to query your databases for matching events or network sessions.
  - From there, you may drill down even further to request session transcripts, copies of the packets or do further searches on other addresses that show up.

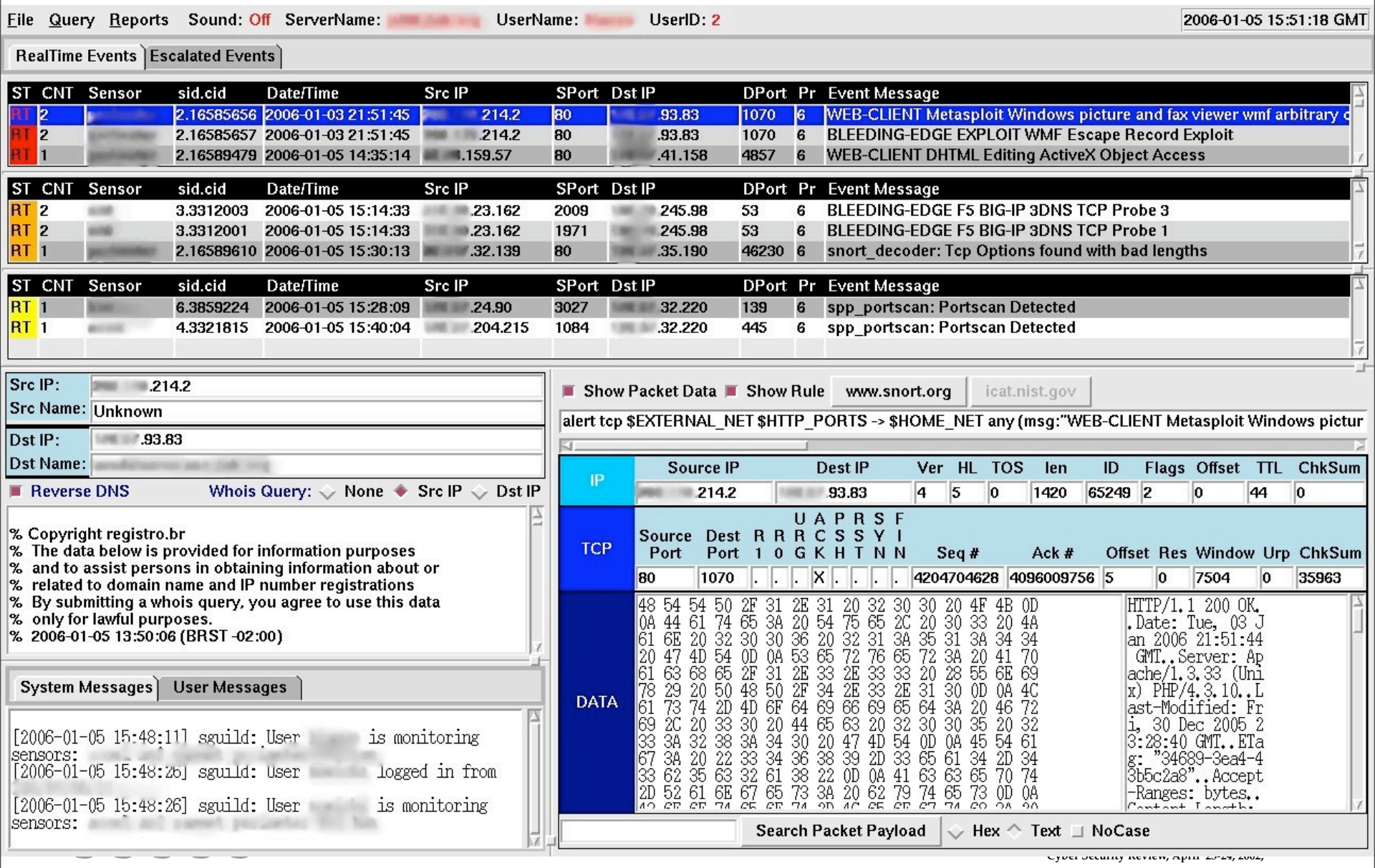
Sguil/NSM Case Study

- Study based on an exploit encountered “in the wild”
- The exploit used the WMF vulnerability
- Delivered via a popunder ad while victim was visiting an otherwise legit website
- This case study recreates my incident research process to show off the power of sguil
- High-level writeup available on my blog:
  - http://infosecpotpourri.blogspot.com/2006/01/how-to-pwn-million-computers-without.html
  - Aimed towards users/managers
- Saved the good stuff for you!

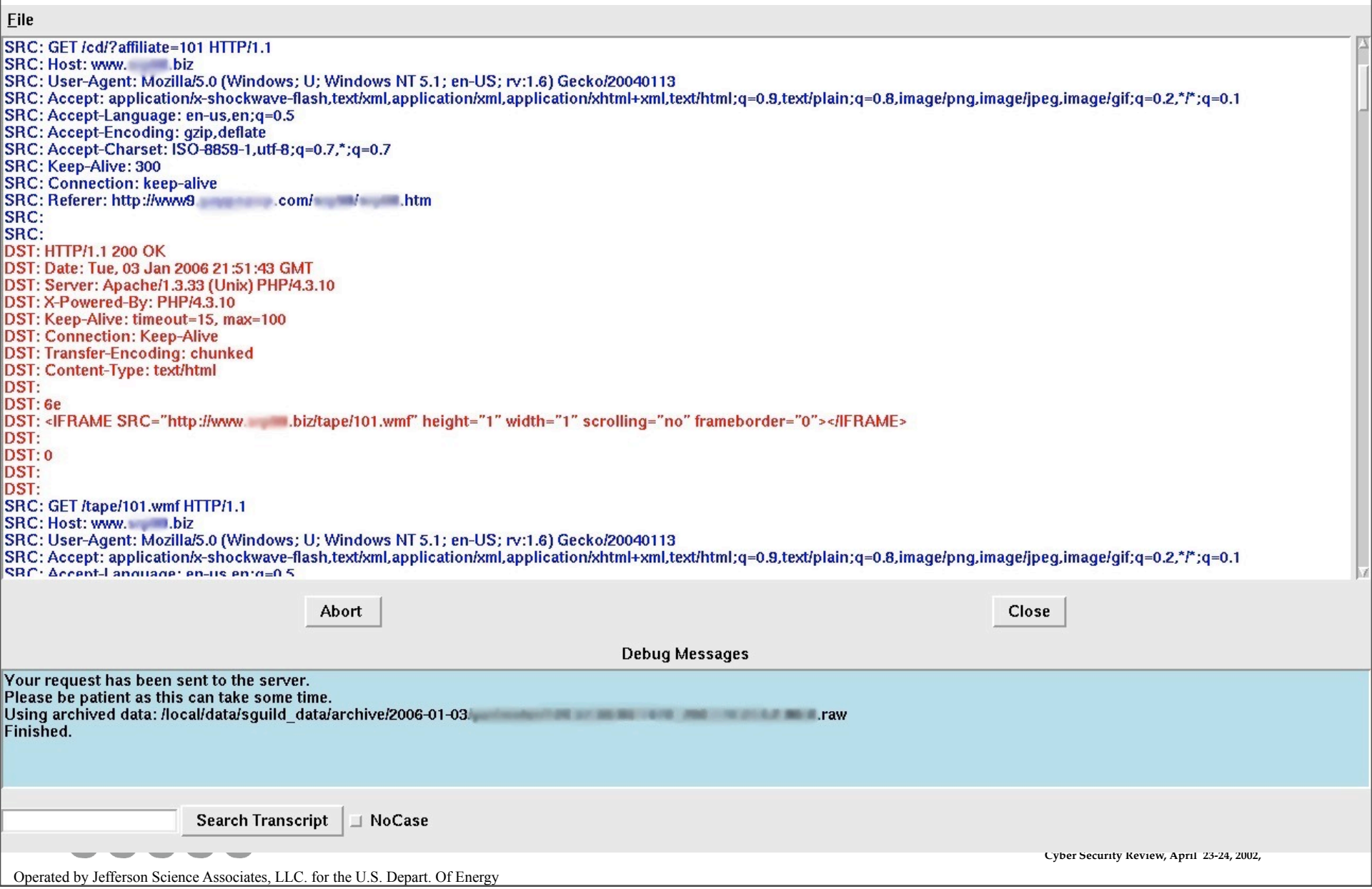
Important Notes

- The victim's identity has been obfuscated to protect the innocent
- The ad servers' identities have been obfuscated to protect the guilty and the not-so-guilty
- Some URLs have been obfuscated to protect the silly
- Legitimate website names appearing in this presentation have nothing to do with this exploit and are only there to provide context for understanding the web session

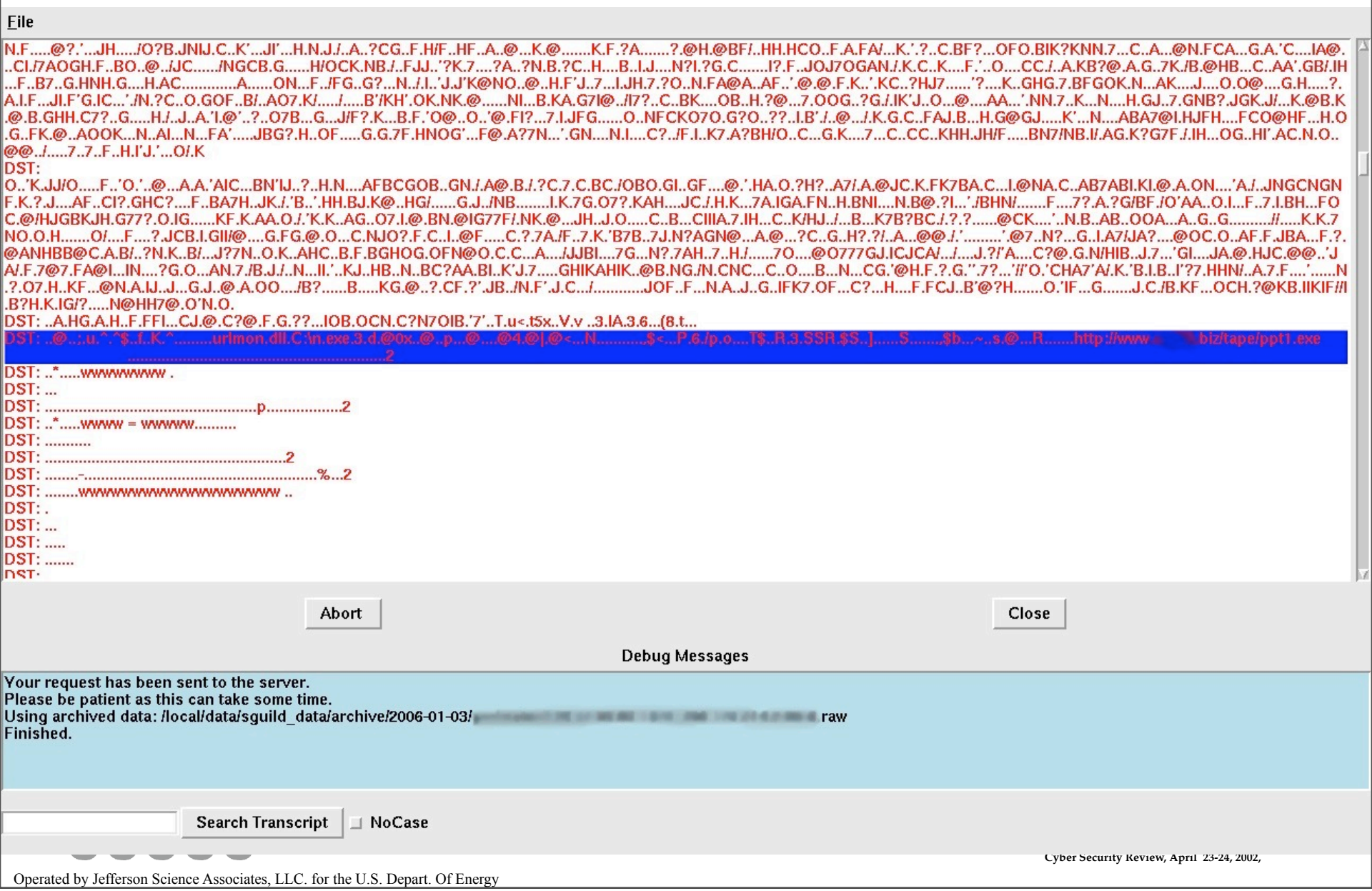
“It was a dark and stormy night…”



Was that a real exploit I just saw?



Was that a real exploit I just saw?



What other events were generated?

File Query Reports Sound: Off ServerName: UserName: UserID: 2 2006-01-05 15:54:56 GMT

RealTime Events | Escalated Events | Event Query 2

Close | Export | WHERE event.timestamp > '2005-12-29' AND status = 0 and (event.src_ip = INET_ATON('.214.2') OR event.dst_ip = INET_ATON('214.2')) | Submit

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1		2.16585656	2006-01-03 21:51:45	.214.2	80	.93.83	1070	6	WEB-CLIENT Metasploit Windows picture and fax viewer wmf arbitrary co
RT	1		2.16585657	2006-01-03 21:51:45	.214.2	80	.93.83	1070	6	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit
RT	1		4.3320003	2006-01-03 21:51:45	.214.2	80	.93.83	1070	6	WEB-CLIENT Metasploit Windows picture and fax viewer wmf arbitrary co
RT	1		4.3320004	2006-01-03 21:51:45	.214.2	80	.93.83	1070	6	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit

Src IP: .214.2
Src Name: Unknown
Dst IP: .93.83
Dst Name:

Reverse DNS | Whois Query: None Src IP Dst IP

```
% Copyright registro.br
% The data below is provided for information purposes
% and to assist persons in obtaining information about or
% related to domain name and IP number registrations
% By submitting a whois query, you agree to use this data
% only for lawful purposes.
% 2006-01-05 13:50:06 (BRST -02:00)
```

System Messages | User Messages

```
connected
[2006-01-05 15:53:05] sguild:
connected
[2006-01-05 15:53:05] sguild:
connected
[2006-01-05 15:53:05] sguild:
connected
```

Show Packet Data | Show Rule | www.snort.org | icat.nist.gov

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"WEB-CLIENT Metasploit Windows pictur
```

IP

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
.214.2	.93.83	4	5	0	1420	65249	2	0	44	0

TCP

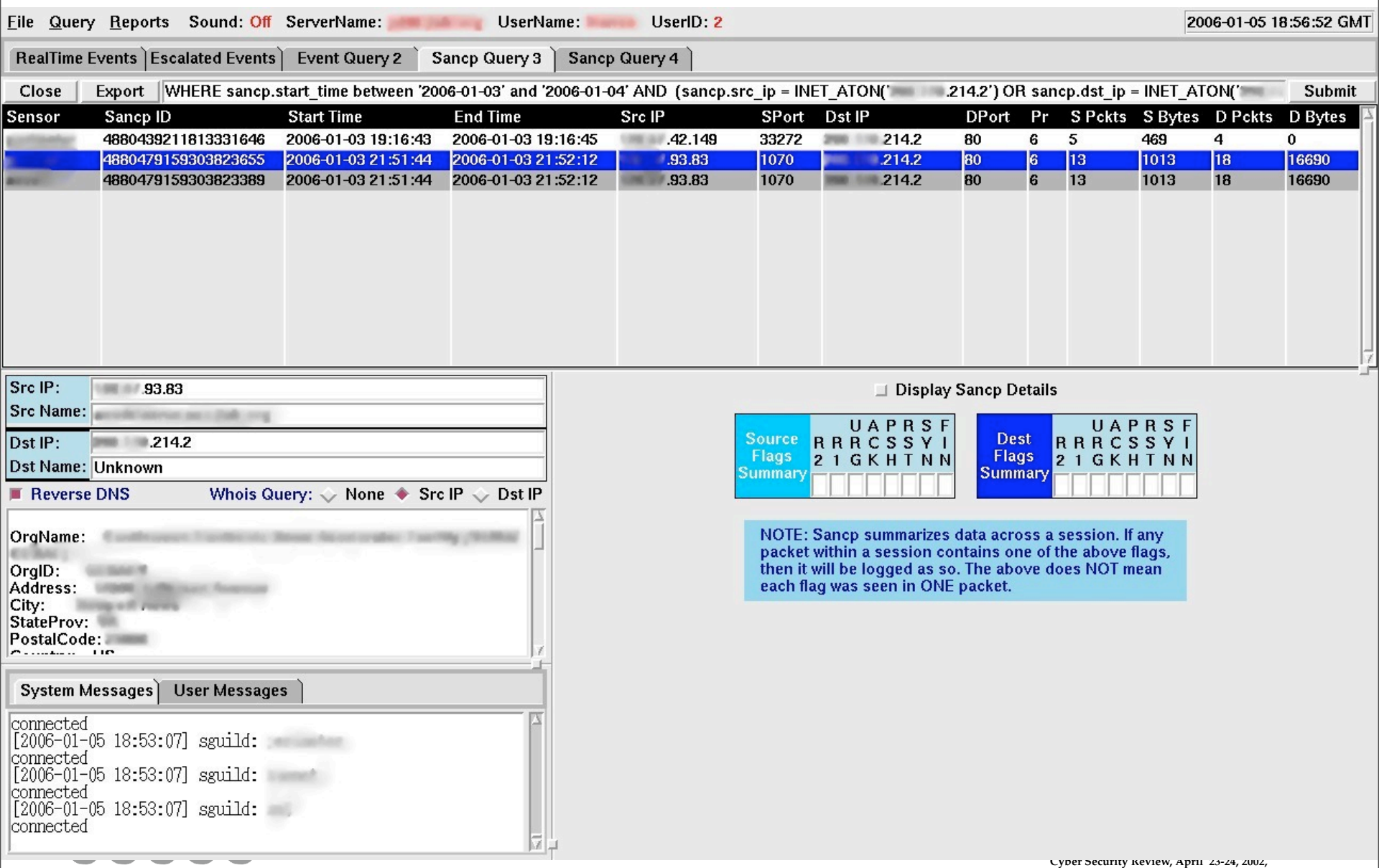
Source Port	Dest Port	R1	R0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
80	1070	.	.	.	X	.	.	.	.	4204704628	4096009756	5	0	7504	0	35963

DATA

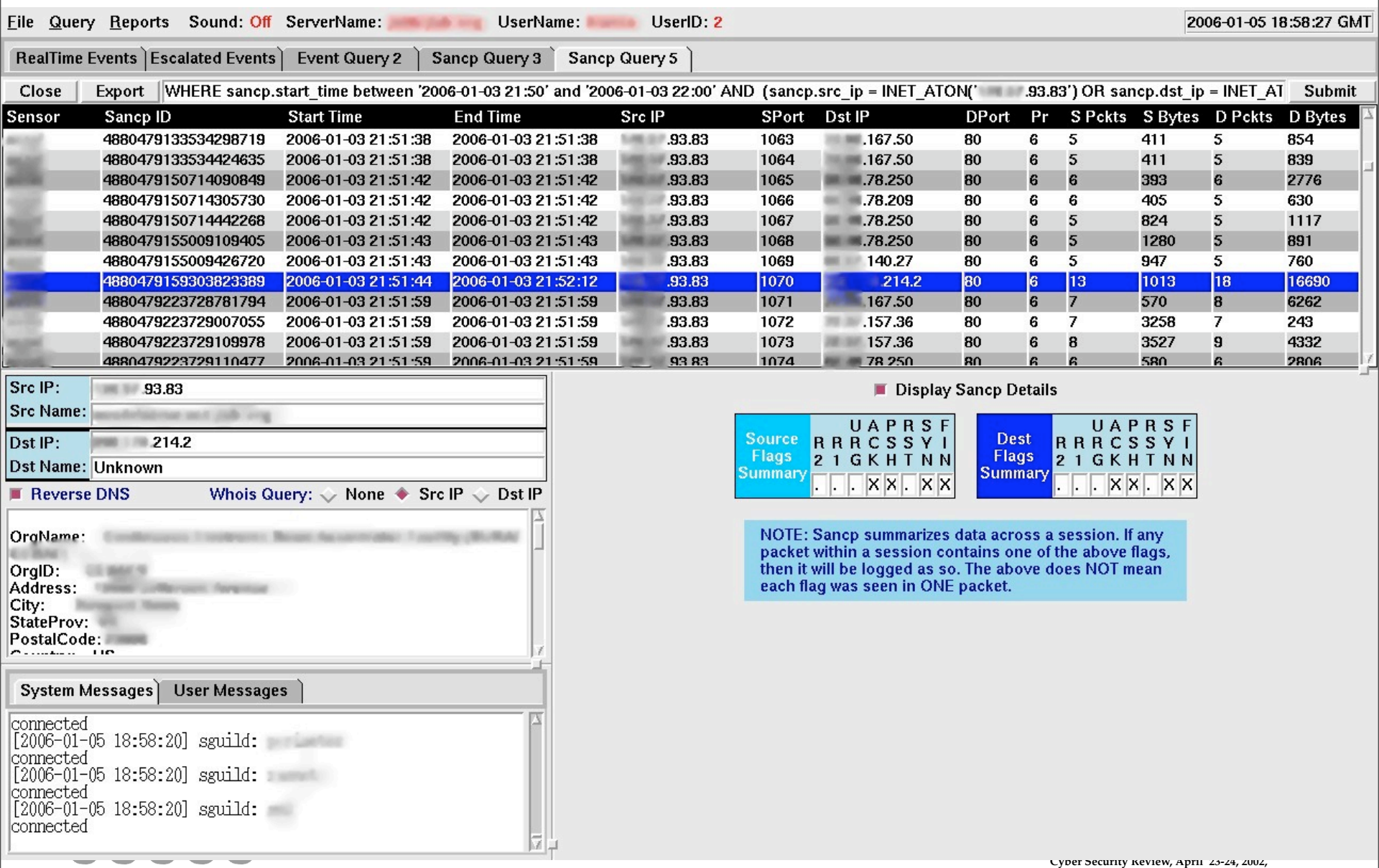
```
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D   HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 54 75 65 2C 20 30 33 20 4A   .Date: Tue, 03 J
61 6E 20 32 30 30 36 20 32 31 3A 35 31 3A 34 34   an 2006 21:51:44
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70    GMT..Server: Ap
61 63 68 65 2F 31 2E 33 2E 33 33 20 28 55 6E 69   ache/1.3.33 (Uni
78 29 20 50 48 50 2F 34 2E 33 2E 31 30 0D 0A 4C   x) PHP/4.3.10..L
61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20 46 72   ast-Modified: Fr
69 2C 20 33 30 20 44 65 63 20 32 30 30 35 20 32   i, 30 Dec 2005 2
33 3A 32 38 3A 34 30 20 47 4D 54 0D 0A 45 54 61   3:28:40 GMT..ETa
67 3A 20 22 33 34 36 38 39 2D 33 65 61 34 2D 34   g: "34689-3ea4-4
33 62 35 63 32 61 38 22 0D 0A 41 63 63 65 70 74   3b5c2a8"..Accept
2D 52 61 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A   -Ranges: bytes..
```

Search Packet Payload | Hex Text NoCase

Quick session check (source)



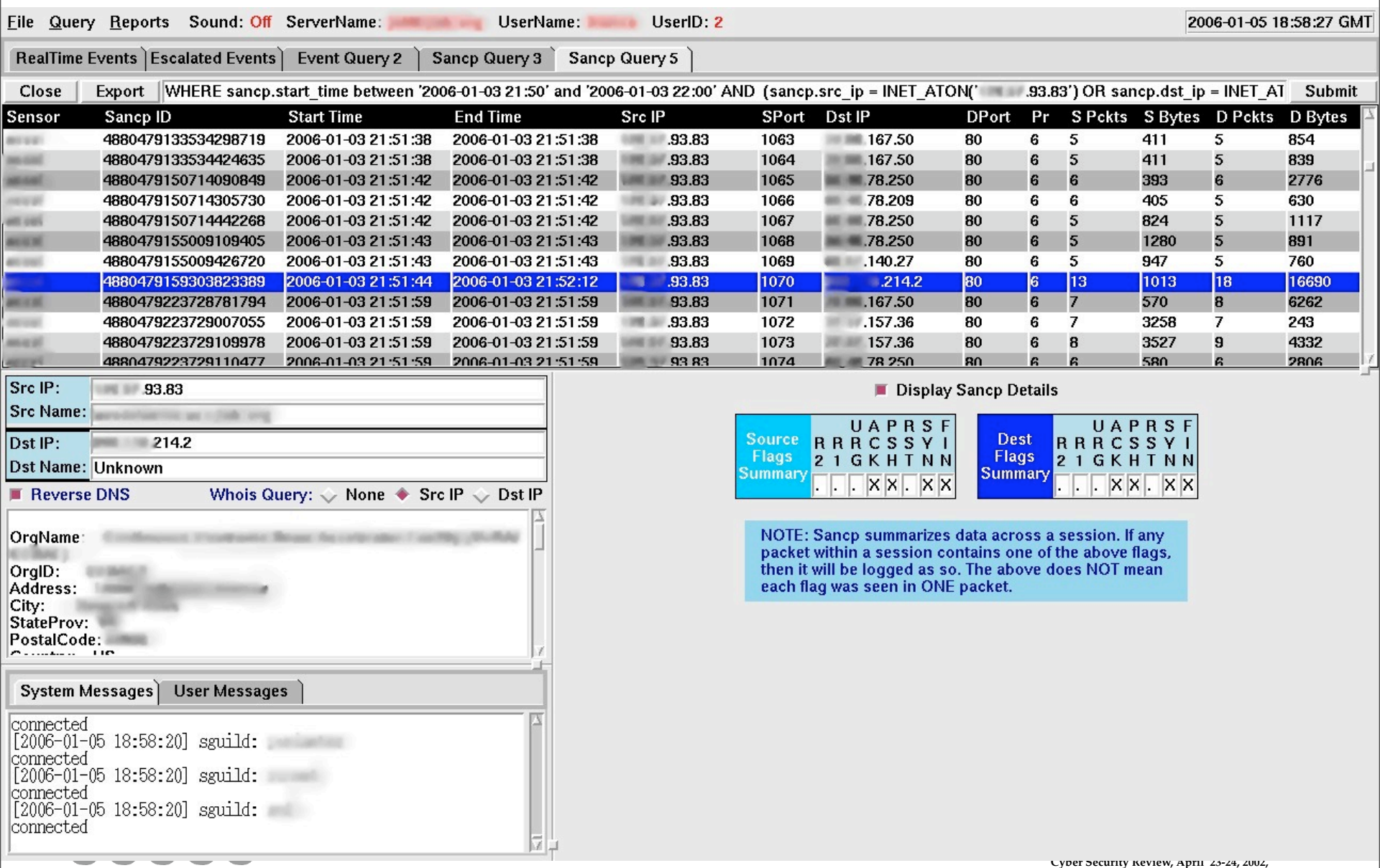
Quick session check (victim)



“I will hunt you down…”

- Also cross-checked other sources, such as:
  - Antivirus logs
  - Manual AV update and scan
  - Checked system for `c:\n.exe` as specified in WMF file
- Exploit attempt seems to have been unsuccessful
- Crisis averted, but let’s have some fun!
- All the sessions are HTTP, so we can leverage that to help us reconstruct the sequence of events
- Begin with the transcript of the exploit session
- Match up “Referrer” tags with requests and work backwards
  - Like climbing a ladder

Victim's Session List



Rung #1: Exploit Delivered

File

```
SRC: GET /tape/101.wmf HTTP/1.1
SRC: Host: www.[redacted].biz
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer: http://www.[redacted] biz/cd/?affiliate=101
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 03 Jan 2006 21:51:44 GMT
DST: Server: Apache/1.3.33 (Unix) PHP/4.3.10
DST: Last-Modified: Fri, 30 Dec 2005 23:28:40 GMT
DST: ETag: "34689-3ea4-43b5c2a8"
DST: Accept-Ranges: bytes
DST: Content-Length: 16036
DST: Keep-Alive: timeout=15, max=99
DST: Connection: Keep-Alive
DST: Content-Type: text/plain
DST:
DST: ......R.....=.....&.....&.....&...#.....TNPP.. ...2.....O.....M.i...
DST: ...&...
DST: .TNPP.....&.....&.....TNPP.....
DST: .....f.....-.....".....-.....-.....!.....-.....-.....".....-.....&.....G.....&.....
DST:
.....-.....&.....JG/.J.AC..B.@/..K.ACI.?..FKJKI.N.7.N.?.J.GO.....BI?..GA.N@N/JO..?...J..BBG...OK..G.B.?.F'.7.C.....B...JFJ..I.O.J.'.....NI@BA7..K.N...J@..J.IK..B//
BC@..KHJ...CK/G.J@7FA.?OGBOJB??'....?/...O./H..IB..AK.'?...@.C.J.J...@.?.I'K...C.C.B.....?/B.@A..CGC.F.?.I?.'.K..C..J..I..HG..CK.I.J...O.'.I..KG/..J...K.H..I.N...?.'.BFJ.G....HFI'FJ.C.....G.J.7
@..O....J.H?7.....7..J.H....N.'.O...../7.N..O.HKB....7..O..NF.'.B'..O@..7/CANAG.GJB.IIN..7K@JH/.@/G?./...G.F.@H.I@O.....I.KAH'..F.7B/'OHAO.IHKC.N..G.....ACH'.B@..A...'/..@.../...../G.7.@.O
' .@@ .E'O .R ' .I / .2EEC@ .E/ .. N' @K / ? A .GA .7 .O ? .2O
```

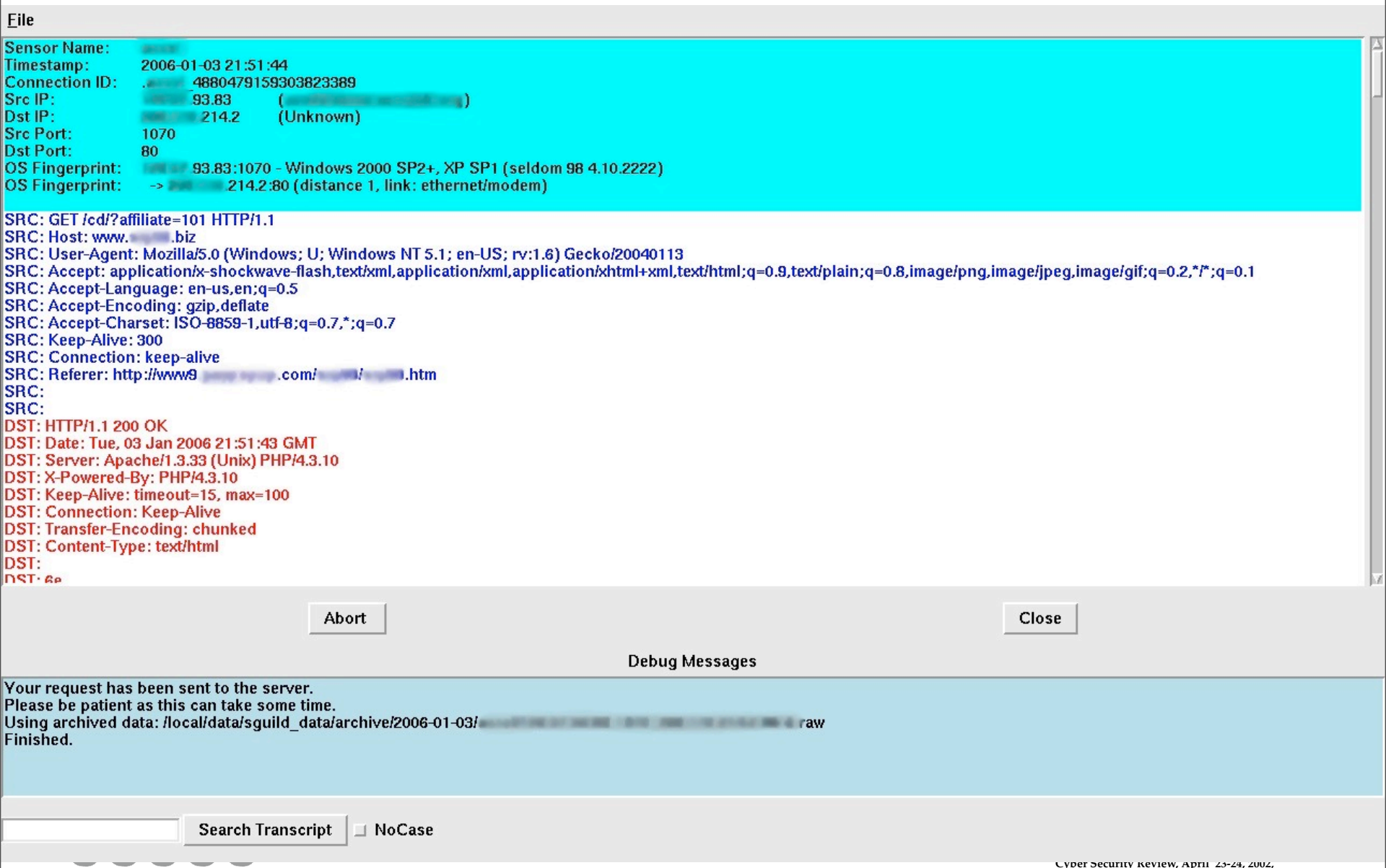
Abort Close

Debug Messages

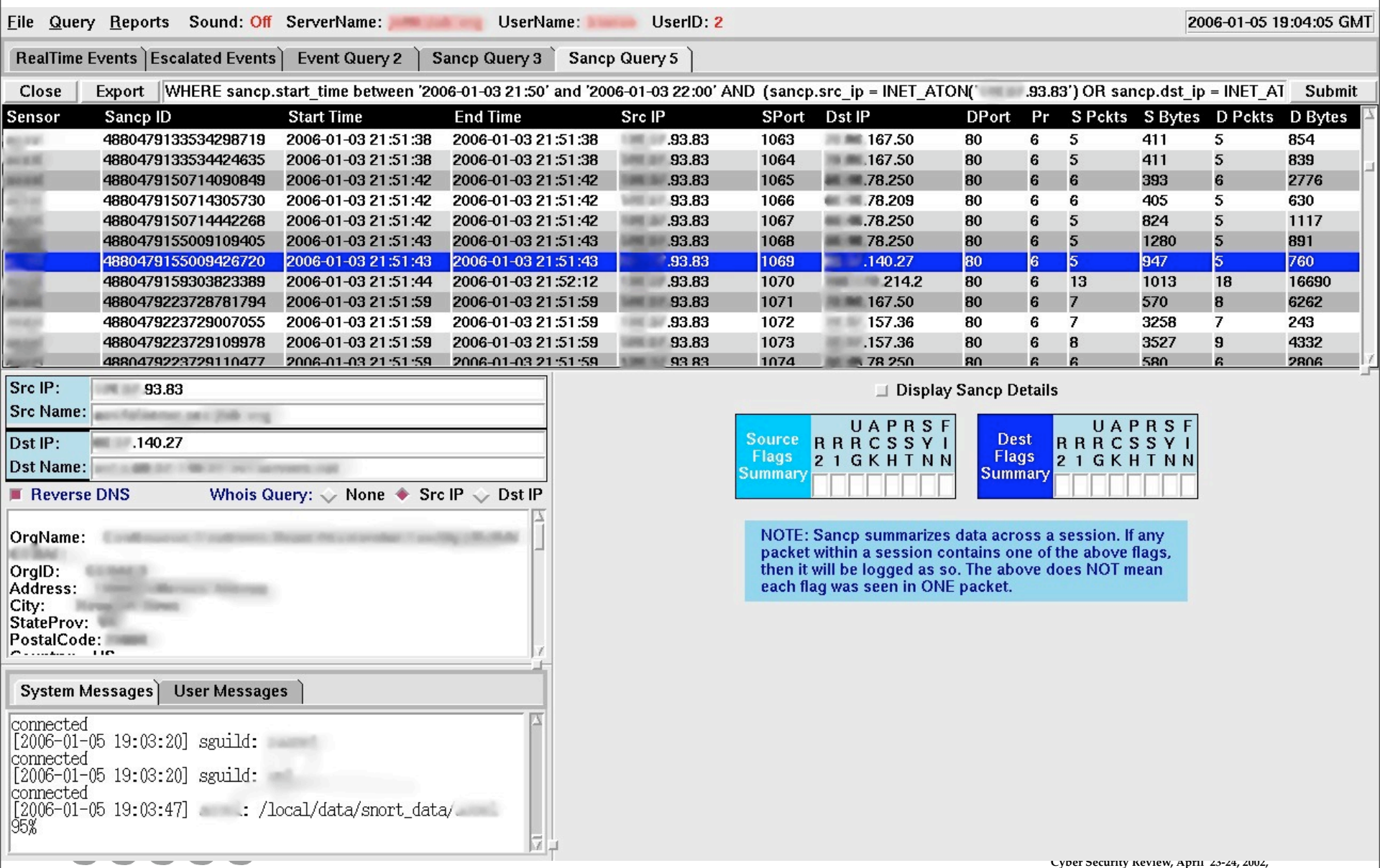
```
Your request has been sent to the server.
Please be patient as this can take some time.
Using archived data: /local/data/sguild_data/archive/2006-01-03[redacted].raw
Finished.
```

Search Transcript NoCase

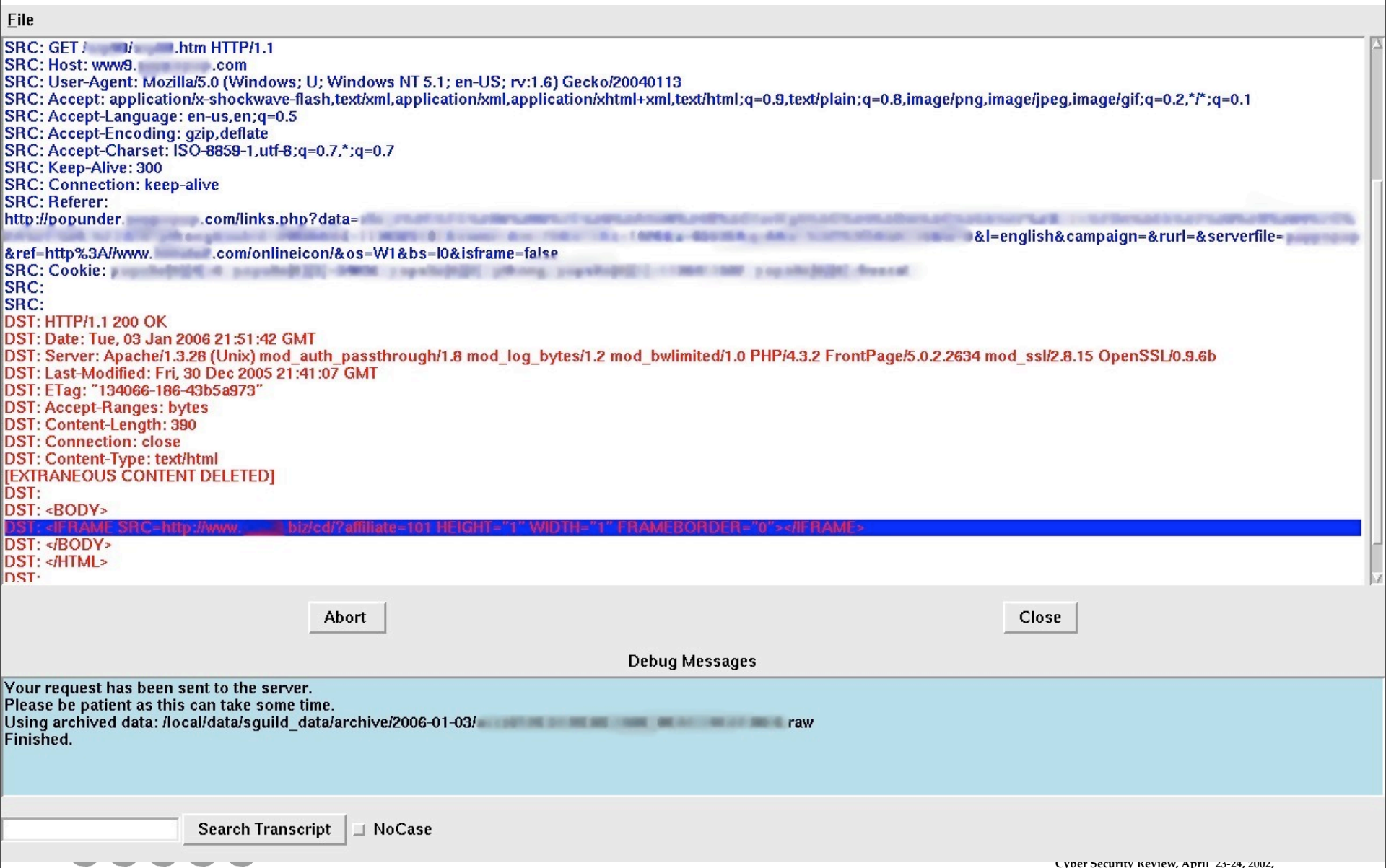
Rung #2: Spf99 Serves the Ad



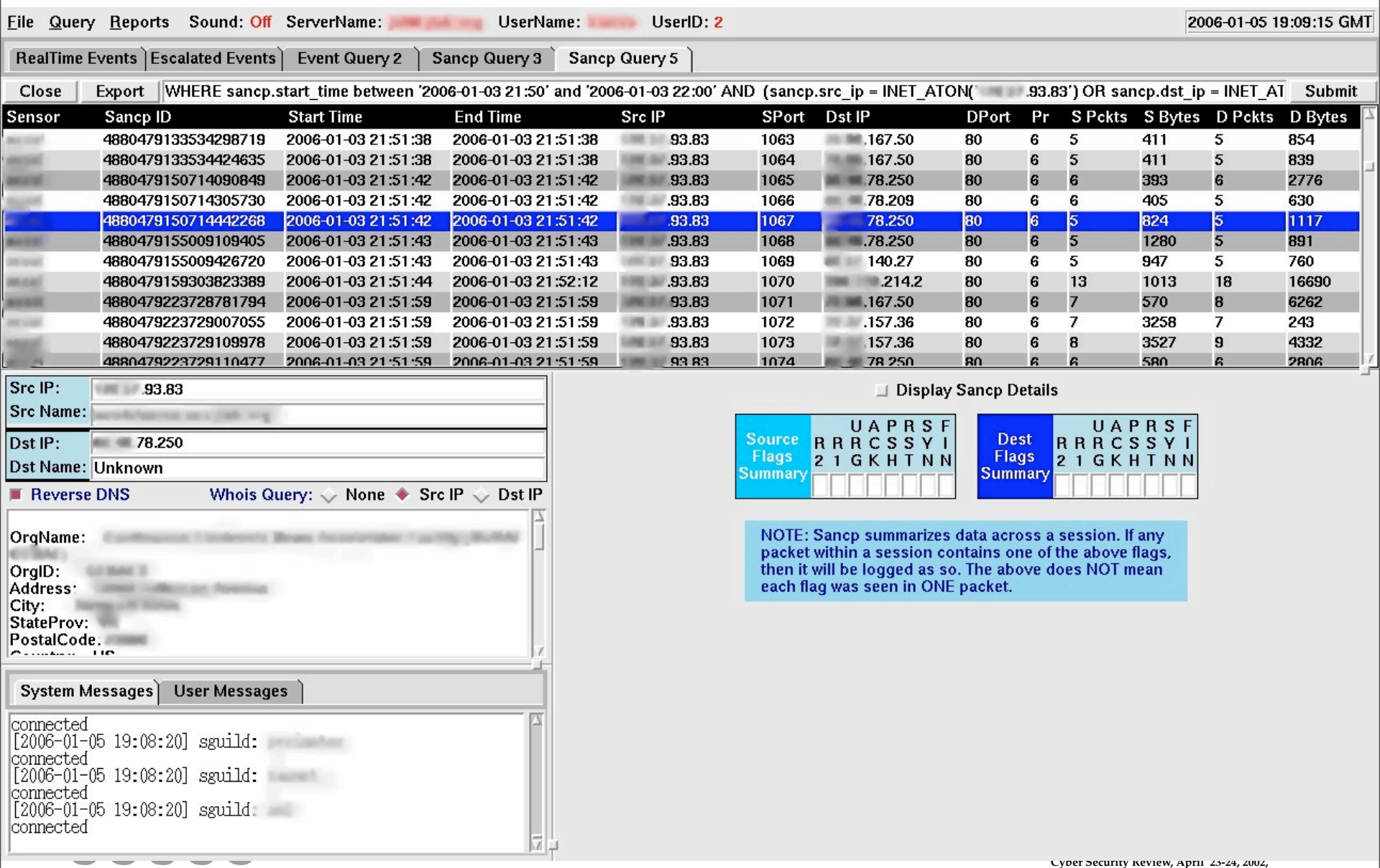
Victim's Session List



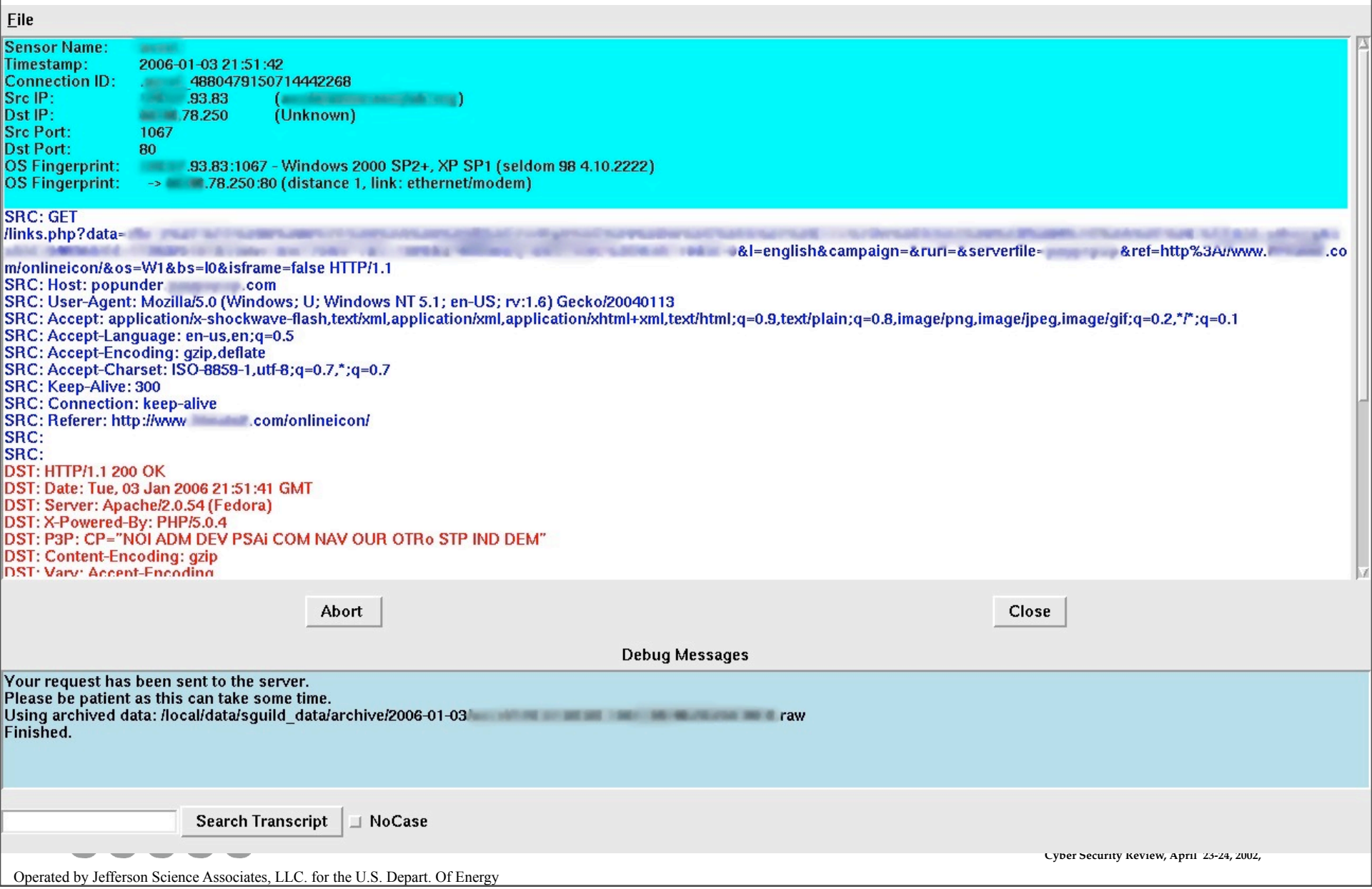
Rung #3: Cash4popupads Handoff



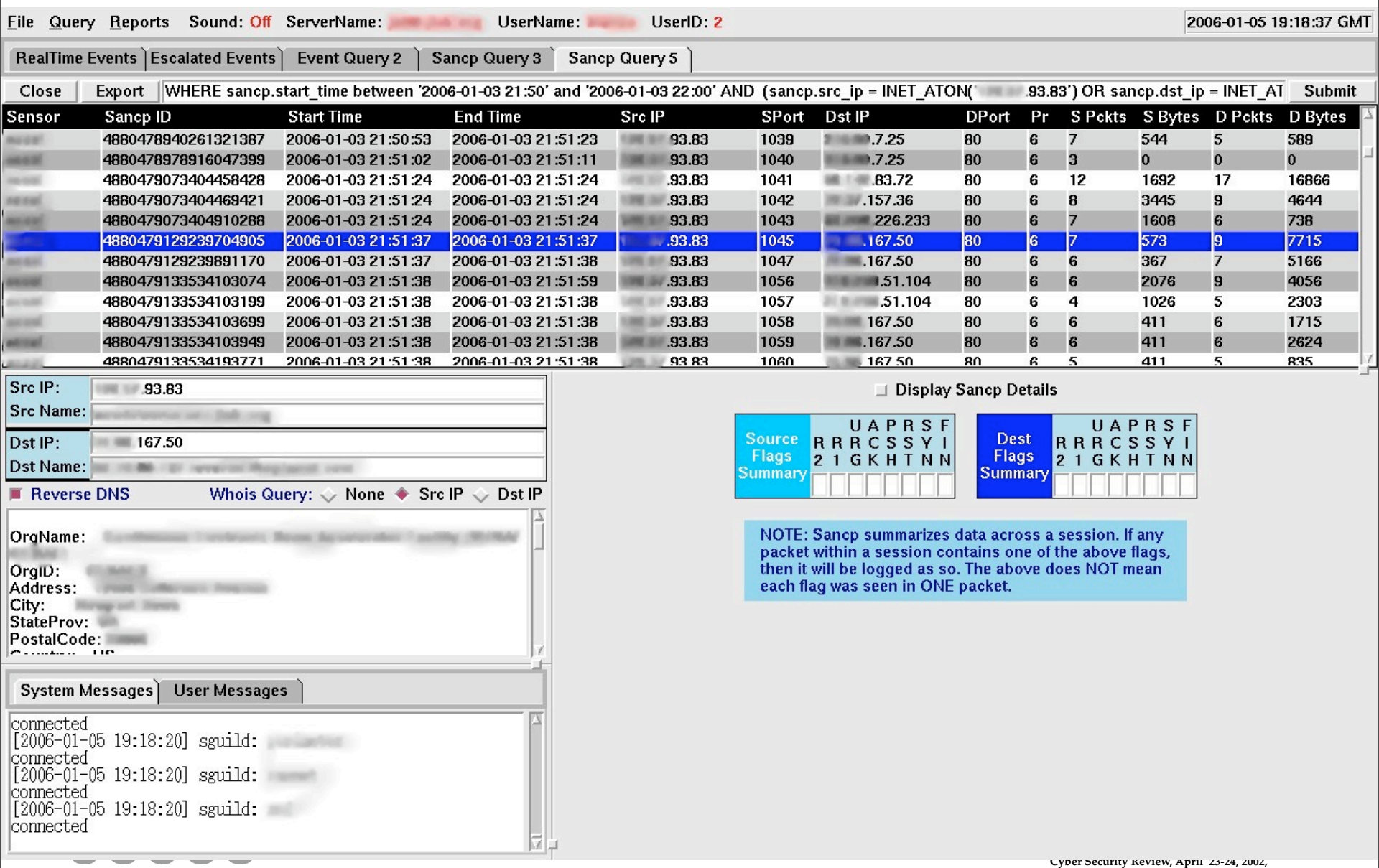
Victim's Session List



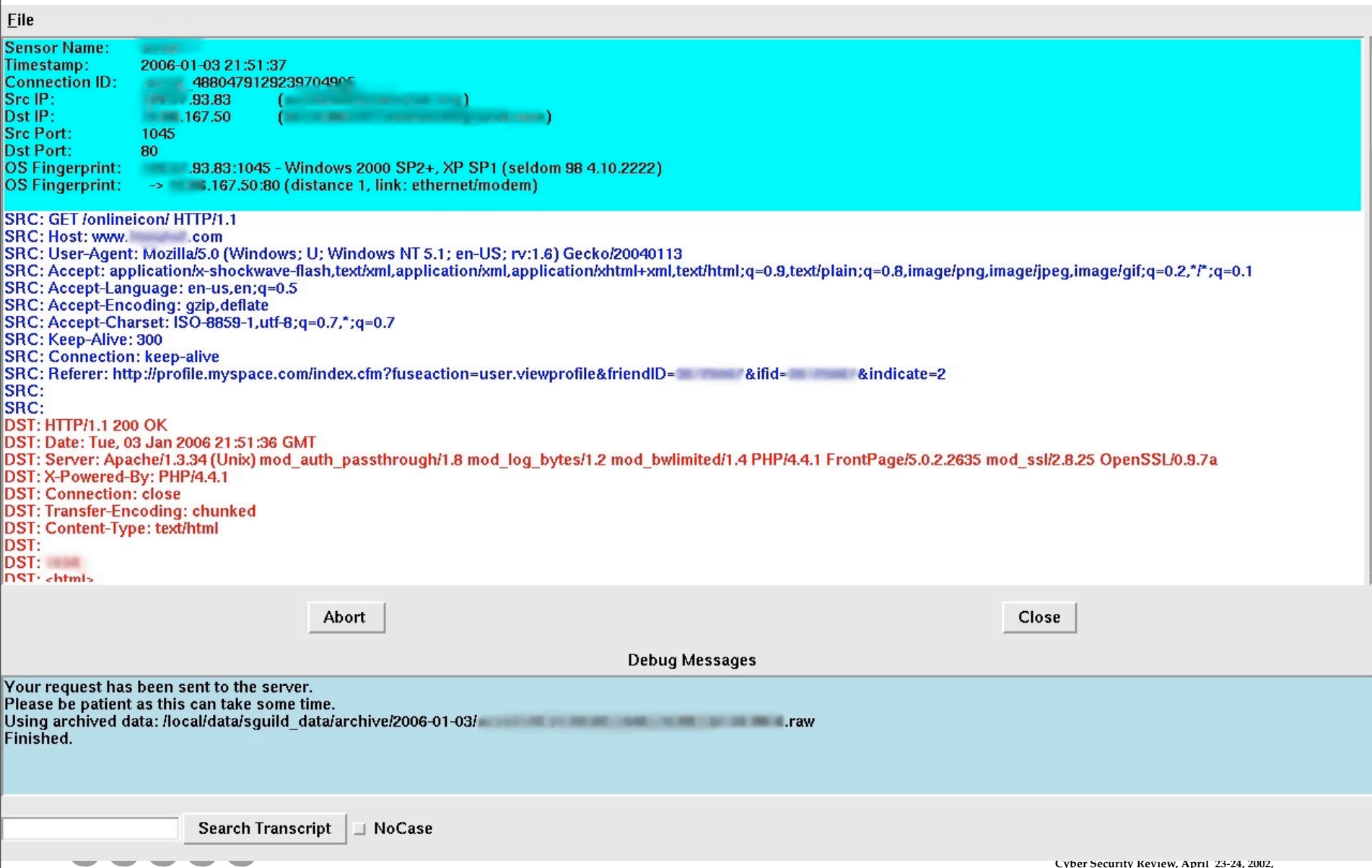
Rung #4: Cash4popupads popunder



Victim's Session List



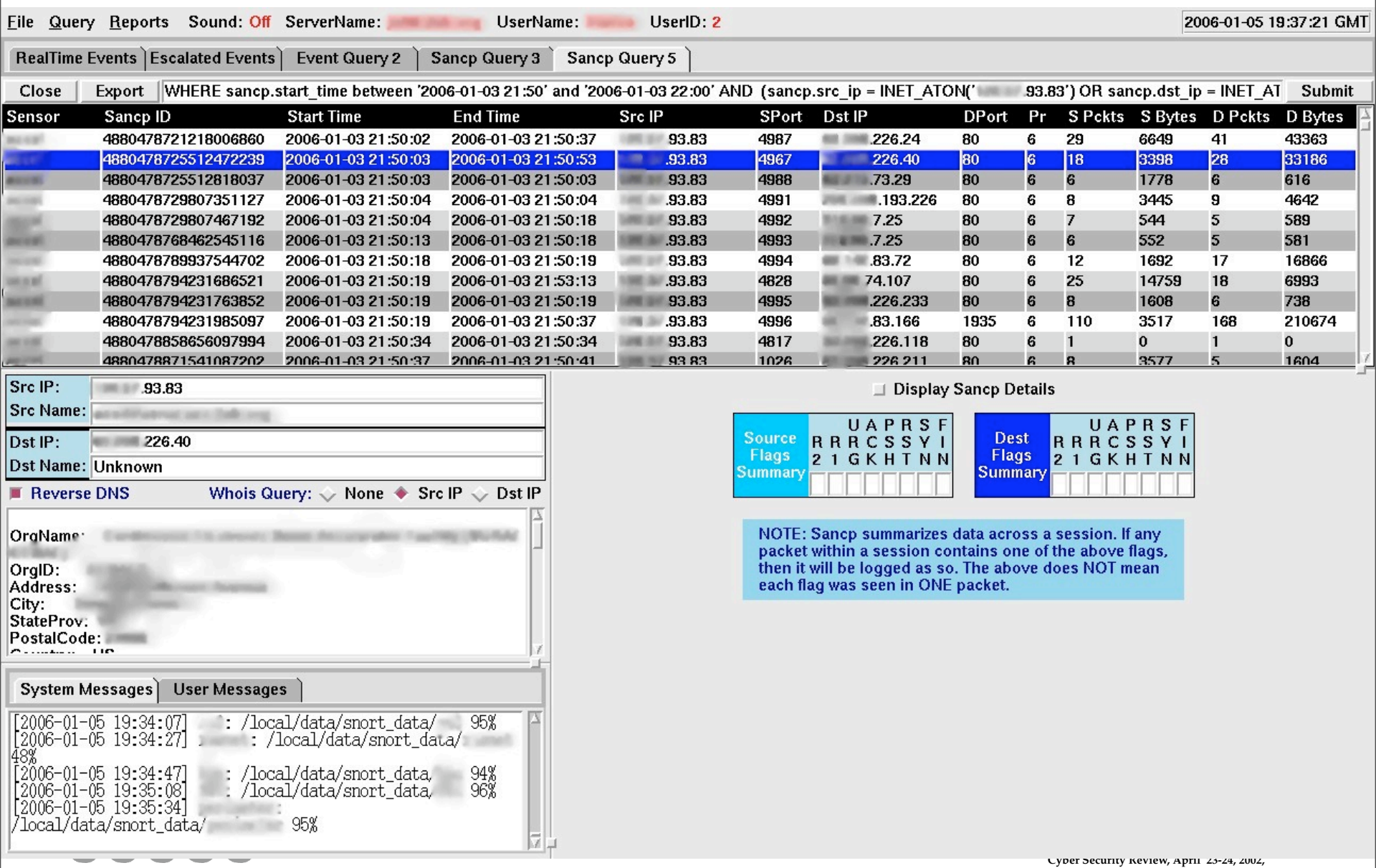
Rung #5: A Legit Site (HTMHelper)



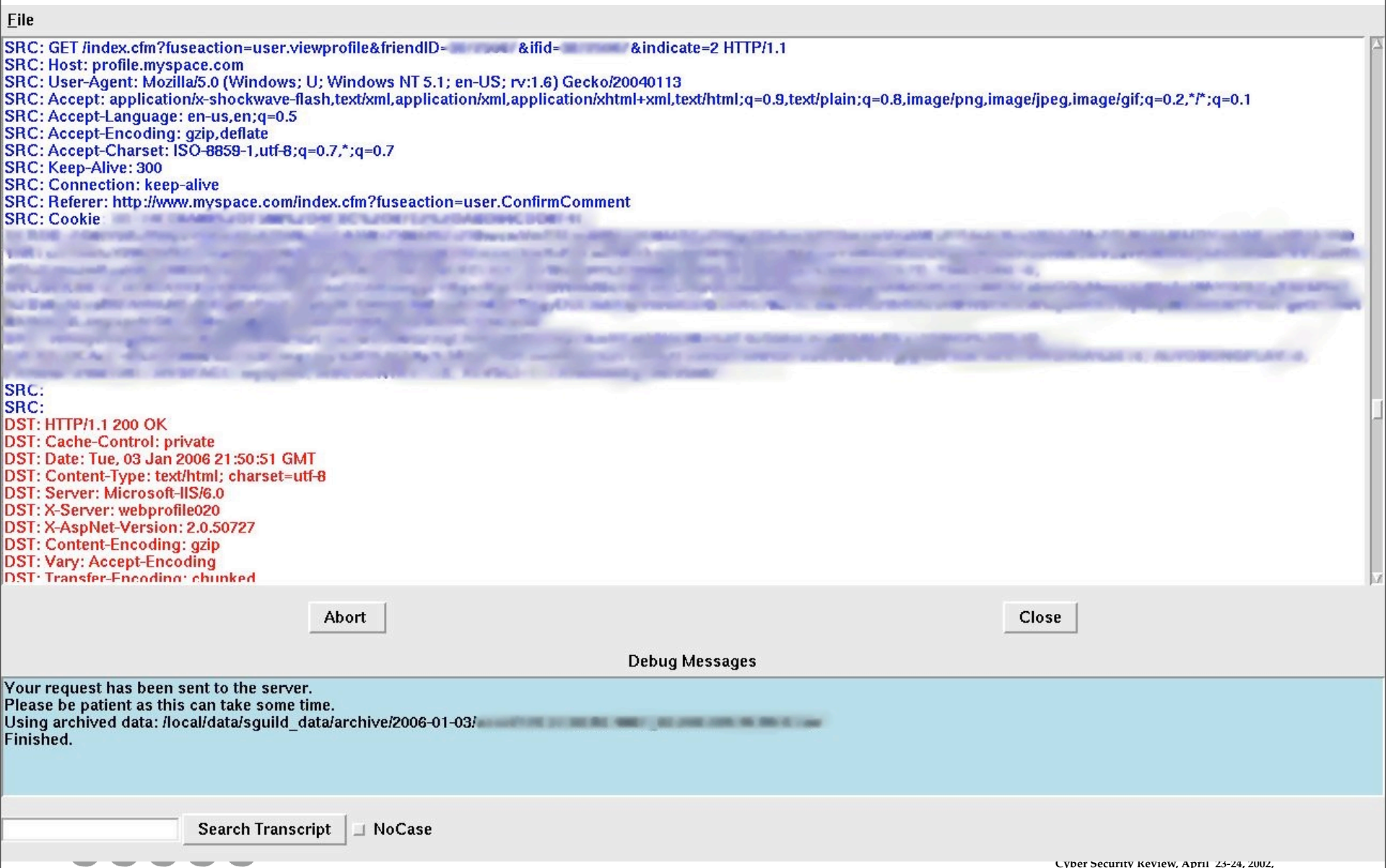
HTMHelper Page Source

```
<!– Cash4popupads.com Advertising Code Begin -->
<SCRIPT LANGUAGE="JavaScript1.1"
SRC="http://popunder.Cash4popupads.com/popup.php?id=XXXX">
</SCRIPT>
<!– Cash4popupads.com Advertising Code End -->
```

Victim's Session List



Rung #6: A Legit Site (MySpace)



MySpace Page Source

```
<div style="position:absolute;
        left:0px;
            top:0px;
            width:88px;
            height:31px;">
<a href="http://www.htmhelper.com/onlineicon/" target="_self">
<img src="http://www.htmhelper.com/onlineicon/clickhere.gif"
    alt="Myspace Online Icon" />
</a>
</div>
```

“Insert Tab A into Slot B…”

- Victim browses a MySpace profile page
  - The page owner or one of the commenters is online, and has the “online status” icon showing by their name.
  - The status icon is provided by and linked back to the HTMHelper site
- The HTMHelper page is ad-supported and contains a JavaScript snippet to display popunder ads from Cash4popupads. This may be annoying, but not intrinsically malicious
- Cash4popupads establishes the popunder window but not the ad content
  - It’s acting more as a conduit for the ads, which are provided by Spf99

“Score along line C and fold…”

- Spf99 served the actual infected file
  - 101.wmf
- Internal codes indicate this was provided by “affiliate 101”
  - Could be an individual
  - Could be another ad network
  - Who knows?
- This is the top of the ladder (for now)
- How would you continue the investigation?

Try It Yourself!

- Download the client-only distribution
  - http://sourceforge.net/projects/sguil
- Log into the server at demo.sguil.net with any username/password.
- Feel free to play around
  - Categorize alerts
  - Request transcripts
  - Search the DB
  - Don’t forget the IRC chat window!

Summary

- NSM is not a replacement for IDS, it's an enhancement
- NSM concentrates on supporting the analyst
  - Increased ability to capture & analyze security data
  - Optimizes for analyst time
  - Despite analyzing more data, increased efficiency means less time and more accurate analysis
- Sguil is the de facto reference implementation
  - Open source
  - Multi-user, multi-platform

NSM with Sguil reduced daily IDS operations time from 5 hours to 45 minutes and resulted in improved detection ability.

More Information

- Sguil project page
  - http://www.sguil.net/
  - http://faq.sguil.net
- Snort website
  - http://www.snort.org/
- Oinkmaster
  - http://oinkmaster.sourceforge.net/
- SANCP
  - http://www.metre.net/sancp.html
- InstantNSM
  - http://instantnsm.sourceforge.net/

Questions?