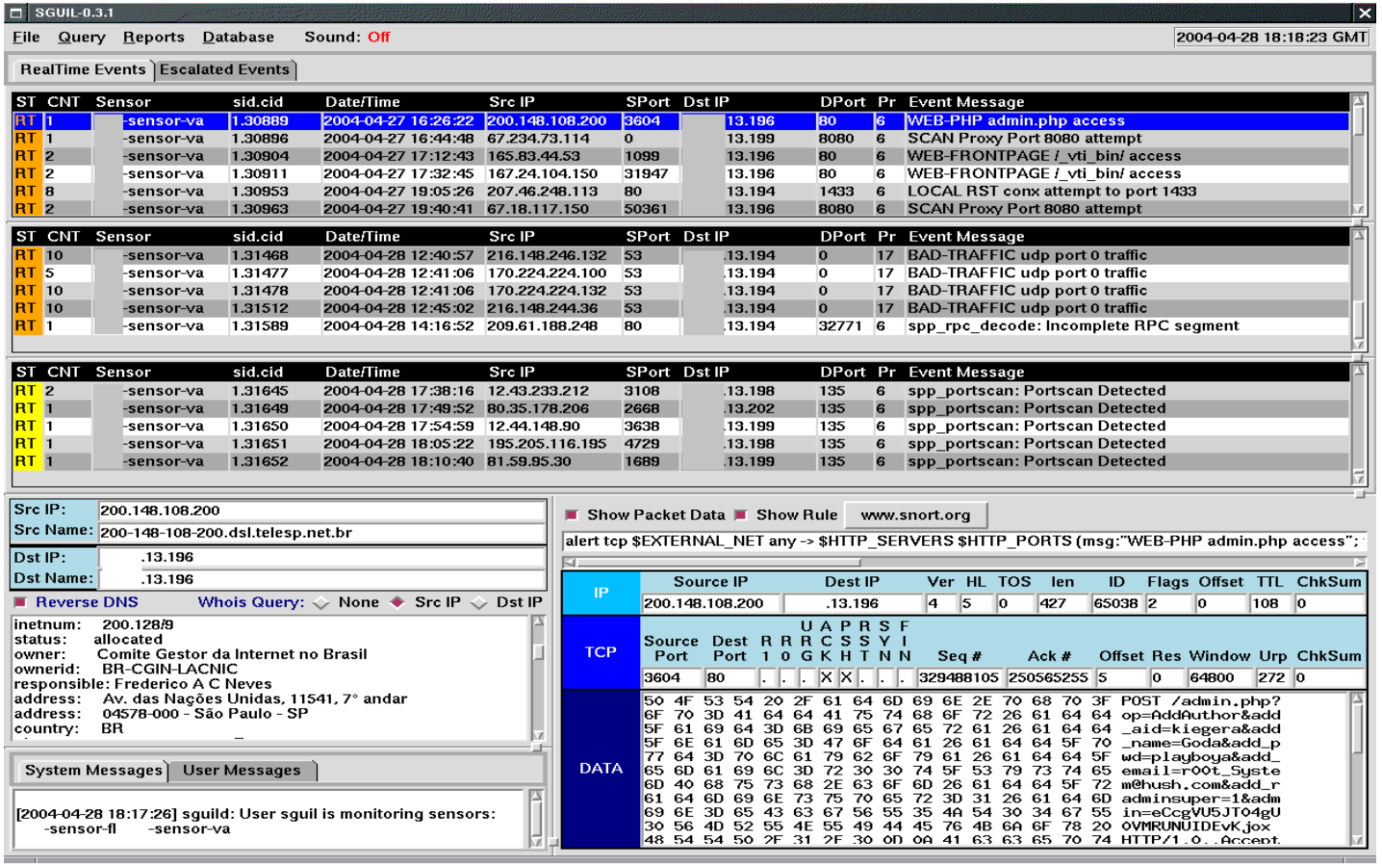
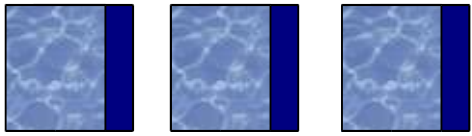
Network Security Monitoring with Sguil



Richard Bejtlich
richard@taosecurity.com
www.taosecurity.com / taosecurity.blogspot.com
BSDCan 14 May 04

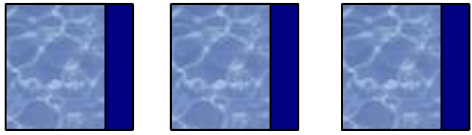
Overview

- Introduction to NSM
- The competition (ACID, etc.)
- Sguil
- Case 1: 403 forbidden
- Case 2: MS-SQL grinding
- Case 3: MS-SQL version overflow attempt
- Case 4: Portscan
- Case 5: Admin-PHP access
- Case 6: SMB grinding
- Case 7: Port 20 to port 20
- Future developments



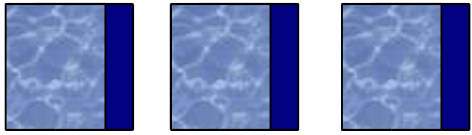
Introduction: My Background

- Hired 1 March 2004 by ManTech Intl. Corp.
- Previously at Foundstone (02-04), Ball Aerospace & Technology Corp (01-02)
- Captain in US Air Force CERT (98-01), trained as intel officer (96-01)
- Author of The Tao of Network Security Monitoring (Addison-Wesley, 800+ pages, due late July 2004)
- Co-author of Real Digital Forensics (Addison-Wesley) with Keith Jones, Curtis Rose (early 2005)



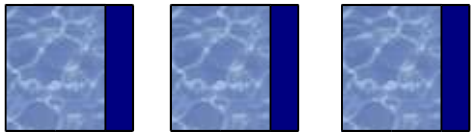
Introduction: Network Security Monitoring

- NSM is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions
- NSM != IDS
- Intrusion detection vendors are alert-focused and consider their job done when they activate the “red blinking light”
- NSM assumes prevention eventually fails and some intruders are smarter than you
- Prepare for the worst by collecting everything you can, technically and legally

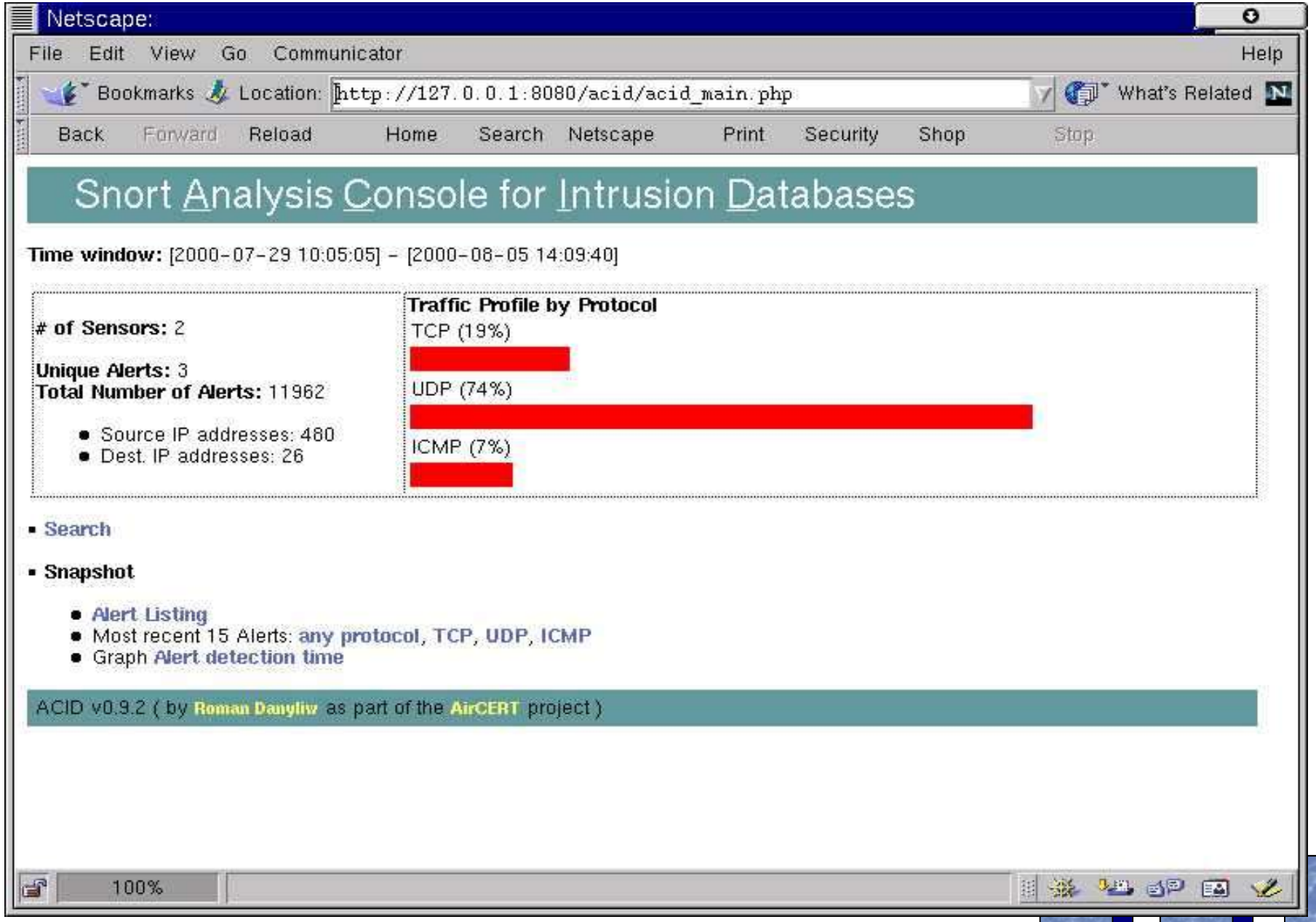


The Competition: ACID, etc.

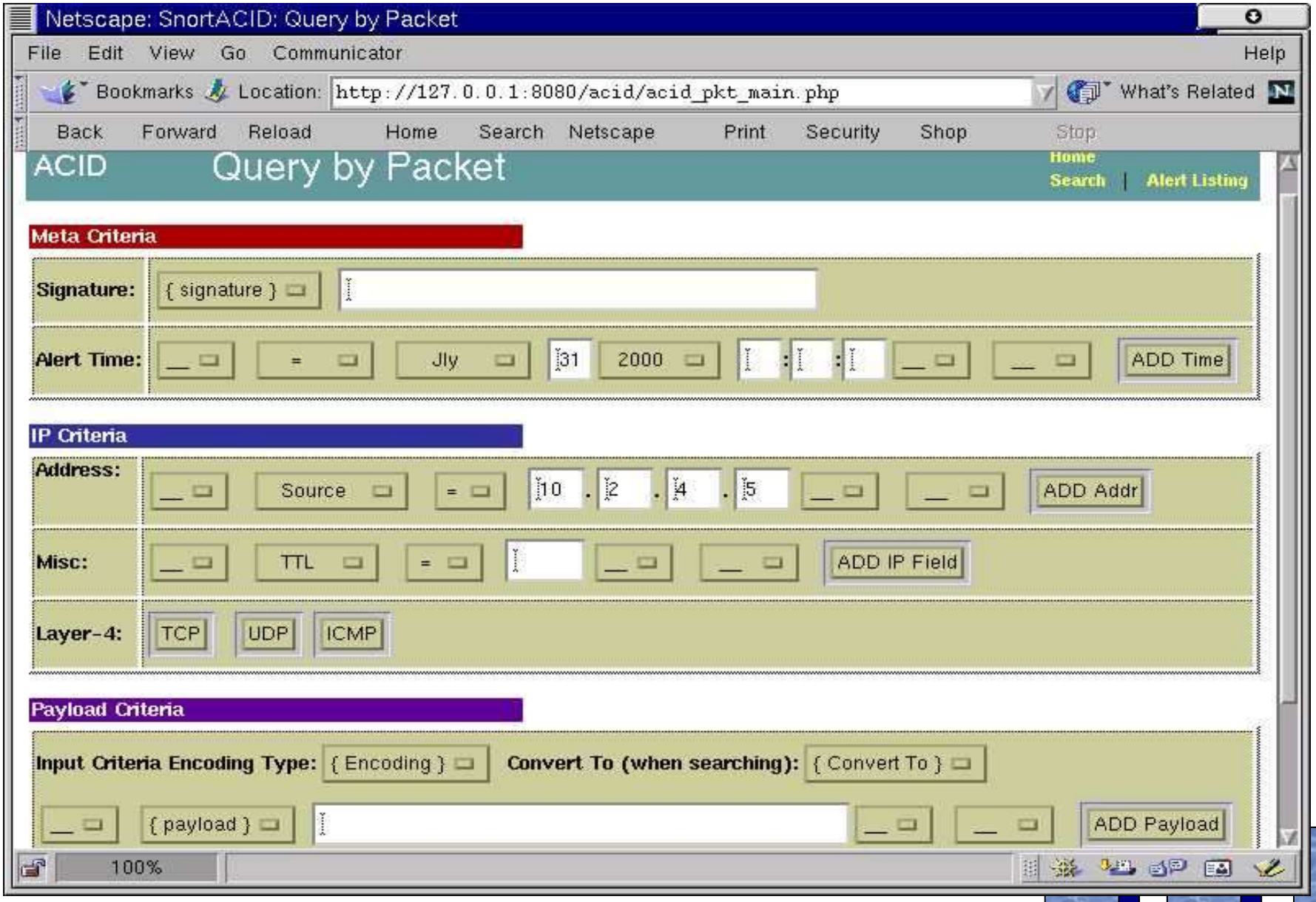
- ACID (acidlabs.sf.net) and the like are Web-based alert browsers
- They only query, display, and store Snort alerts
- Do not give enough information for an analyst to ***make a decision***
- Predominantly consider the number of alerts as a proxy for their severity
- No capability for workflow, alert categorization, analyst responsibility, or information sharing



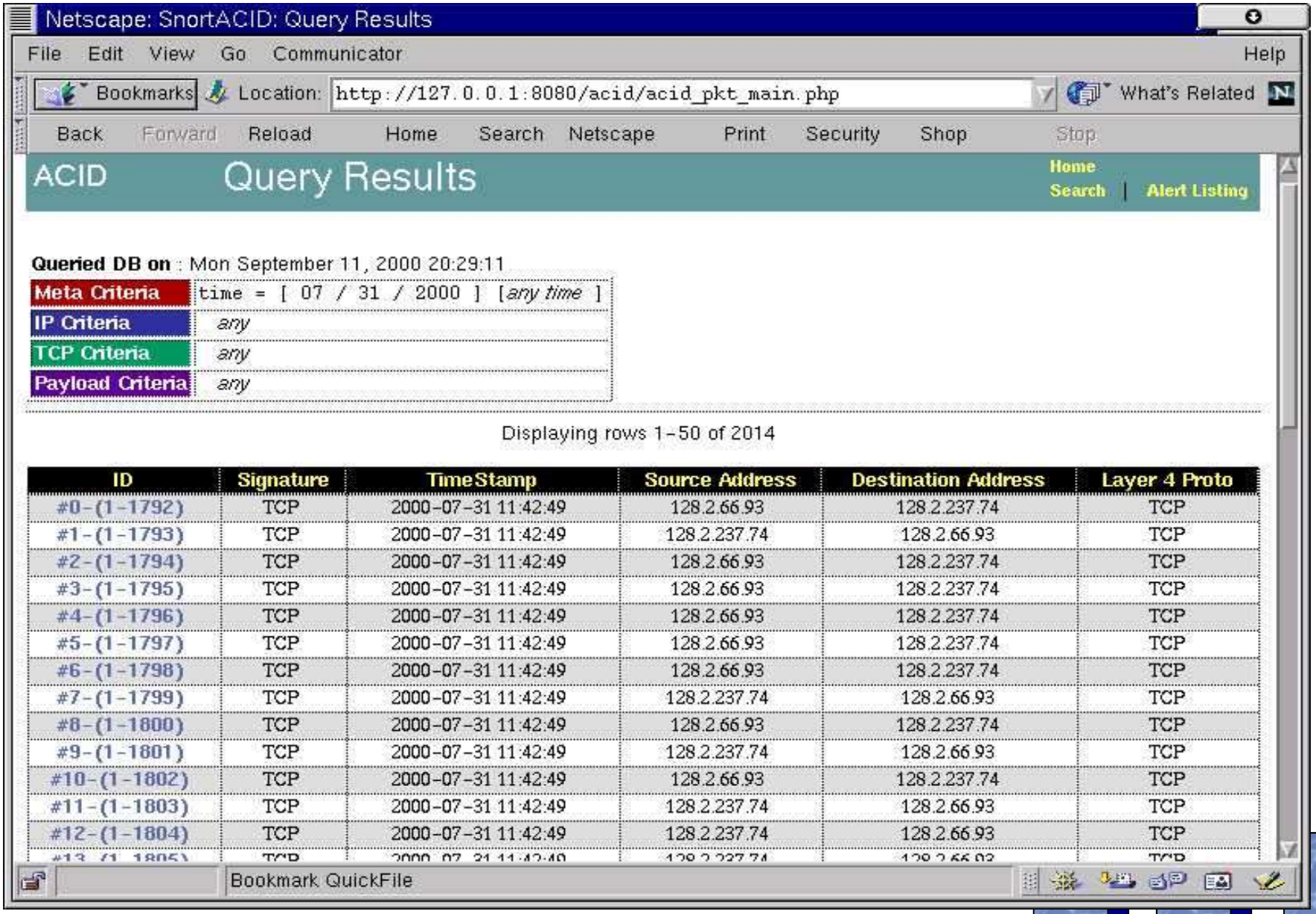
ACID's high count implies 'bad'



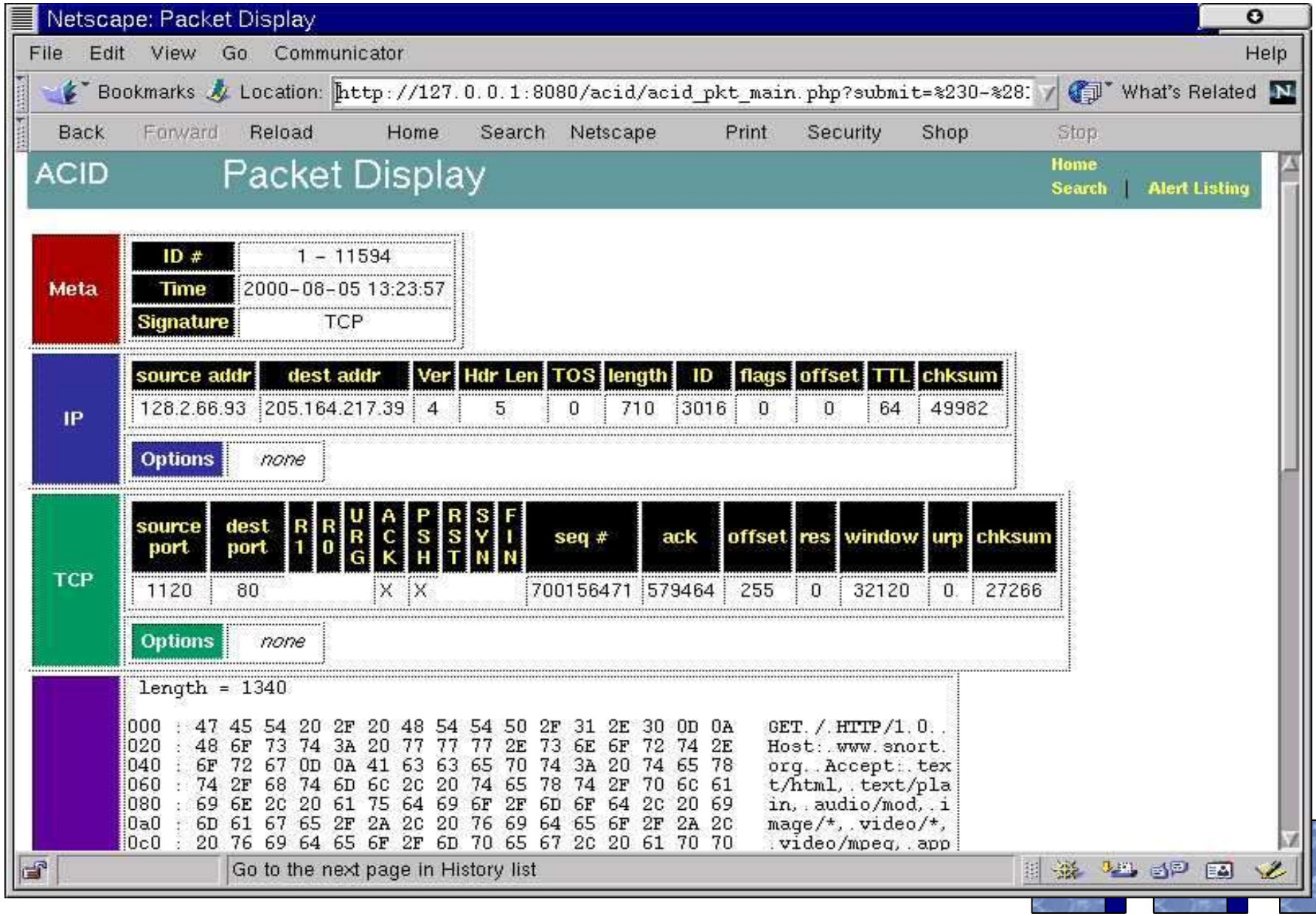
ACID's clunky query screen



ACID's questionable results

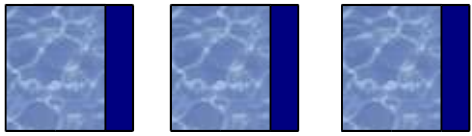


A packet -- so what?



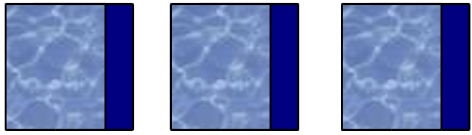
NSM Requirements

- Need to investigate different sorts of events
  - *Normal* activity triggers alerts but is not harmful
  - *Suspicious* activity is unusual but probably not harmful
  - *Malicious* activity is definitely designed to harm targets
- Need supporting data to make decisions
  - *Alert* data provides a potential indicator of security incidents
  - *Session* data is a content neutral summary of transactions
  - *Full content* data captures packet-level details, including application contents
  - *Statistical* data summarizes traffic

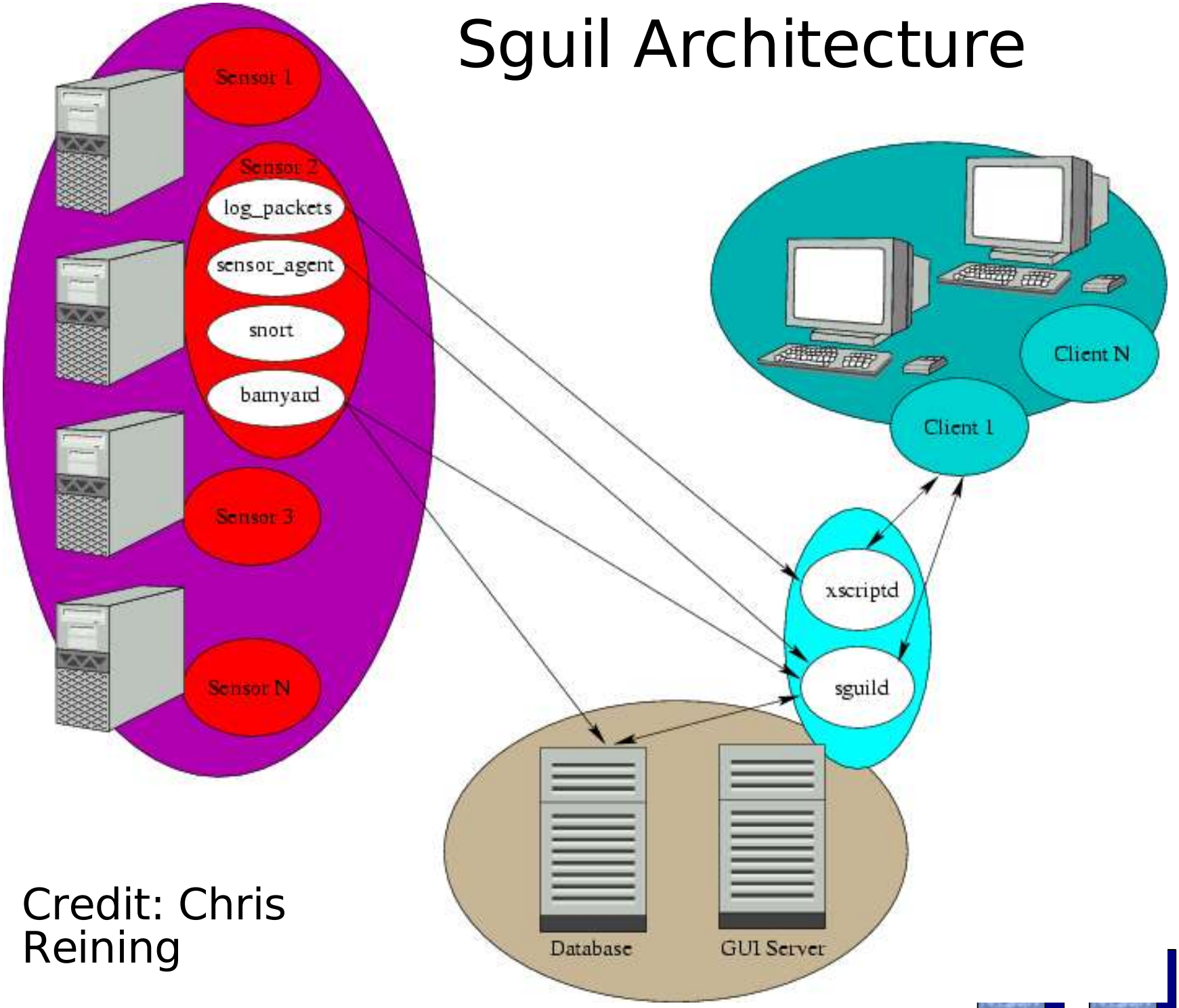


Sguil (sguil.sf.net)

- Sguil is an open source interface for NSM
- Written by Bamm Visscher, mostly in Tcl/Tk (cross-platform, especially the client)
- Consists of components to collect NSM data:
  - Alert data: Snort and Barnyard
  - Session data: SANCP or Snort stream4 keepstats
  - Full content data: Second instance of Snort
  - Statistical data: Nothing formal (yet)
- Detailed install docs for FreeBSD available; Linux, other BSDs work



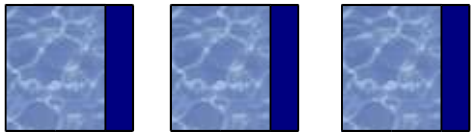
Sguil Architecture

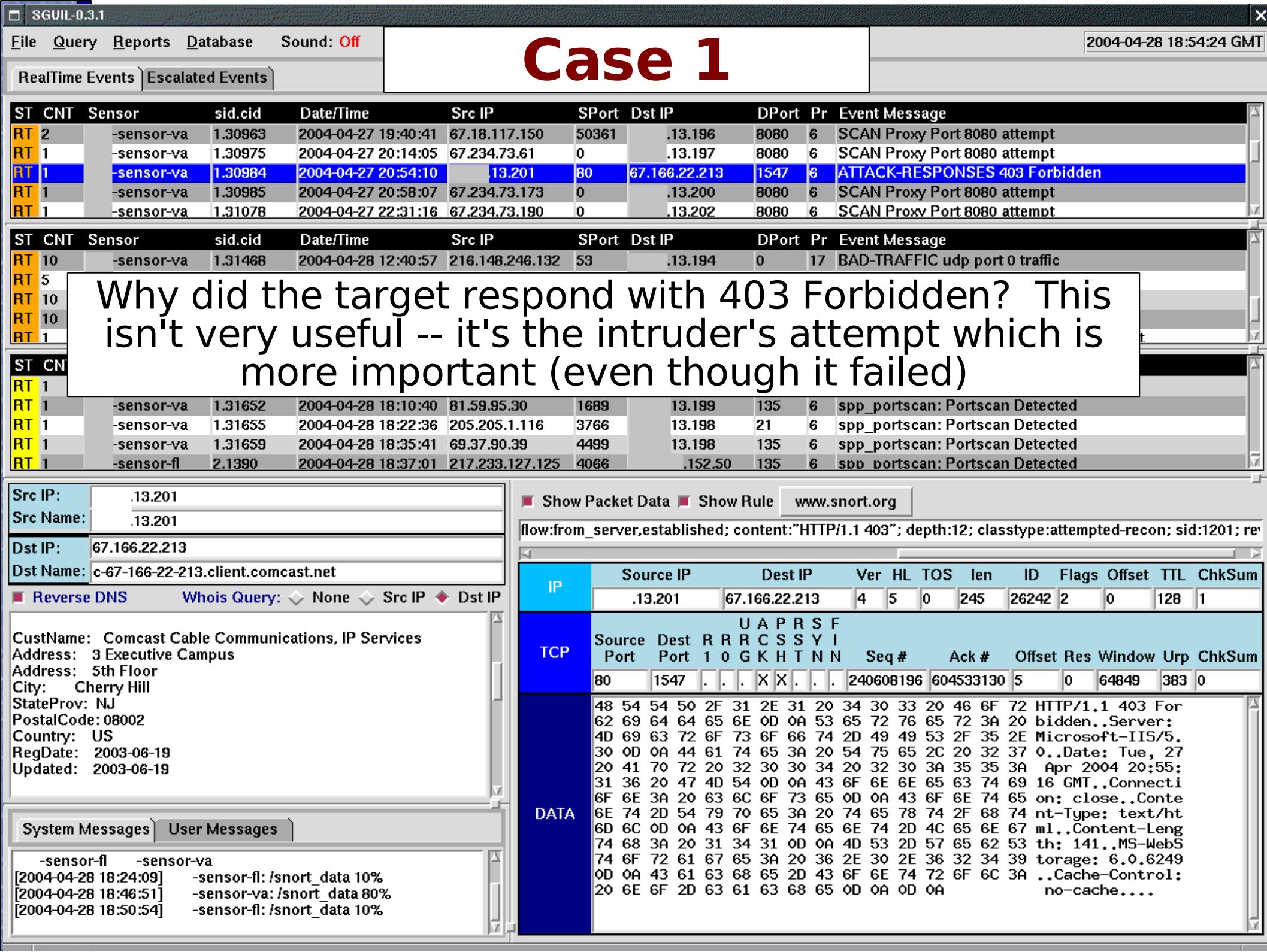


Credit: Chris Reining

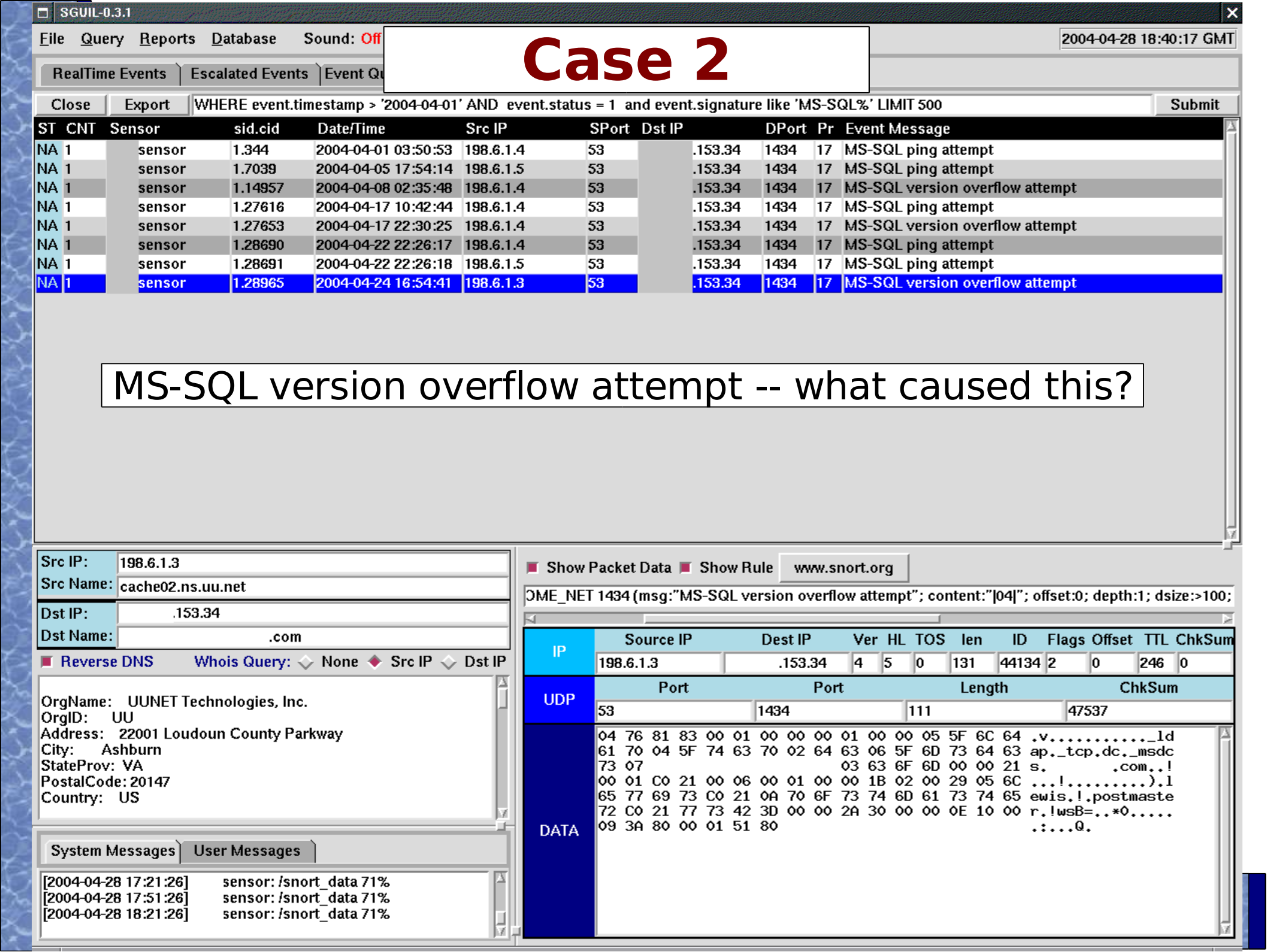
Case studies

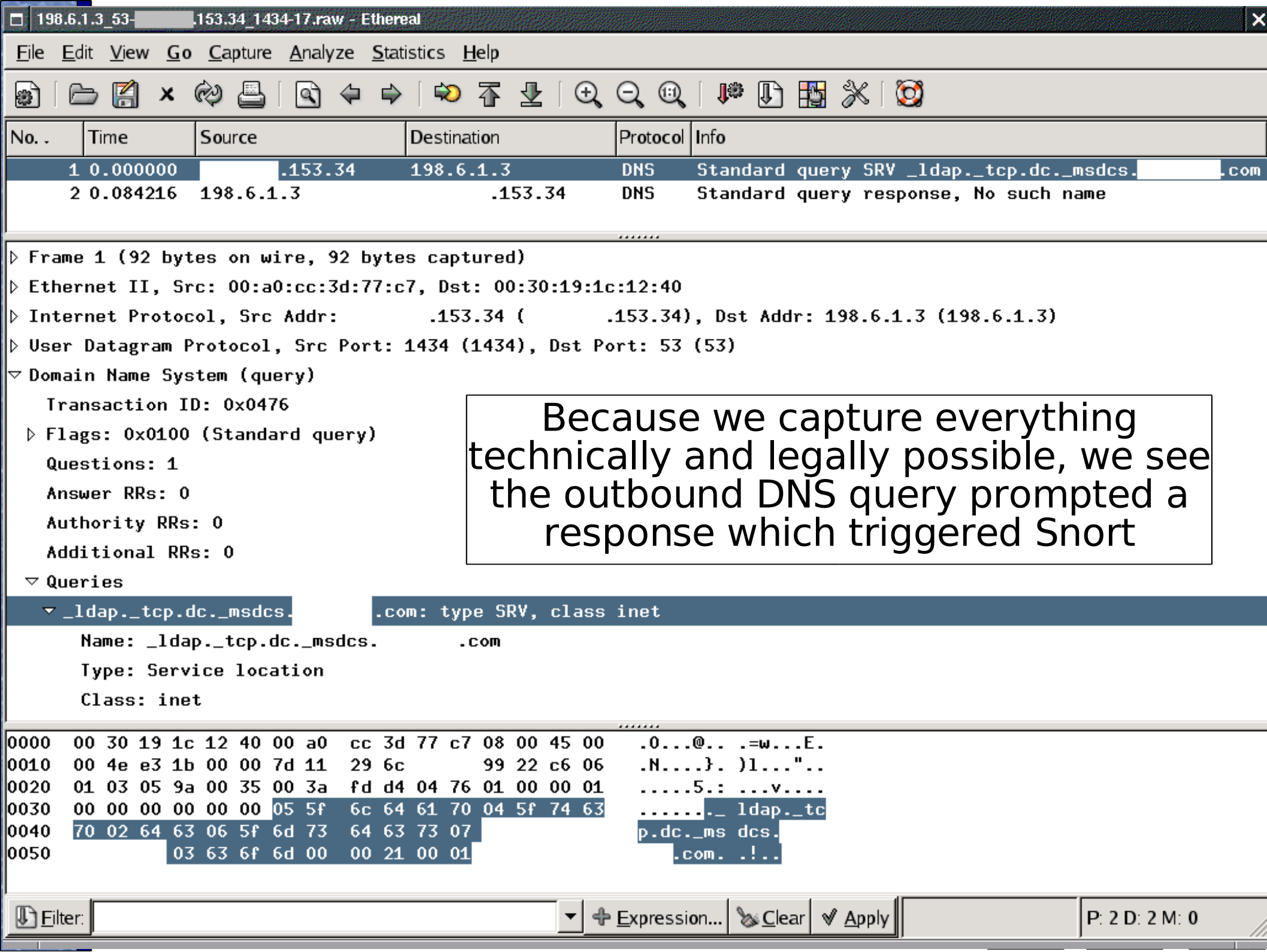
- The following case studies show real data collected during the last few weeks
- Local sensor watches traffic to and from various network perimeters
- Data has been sanitized to remove identifying information

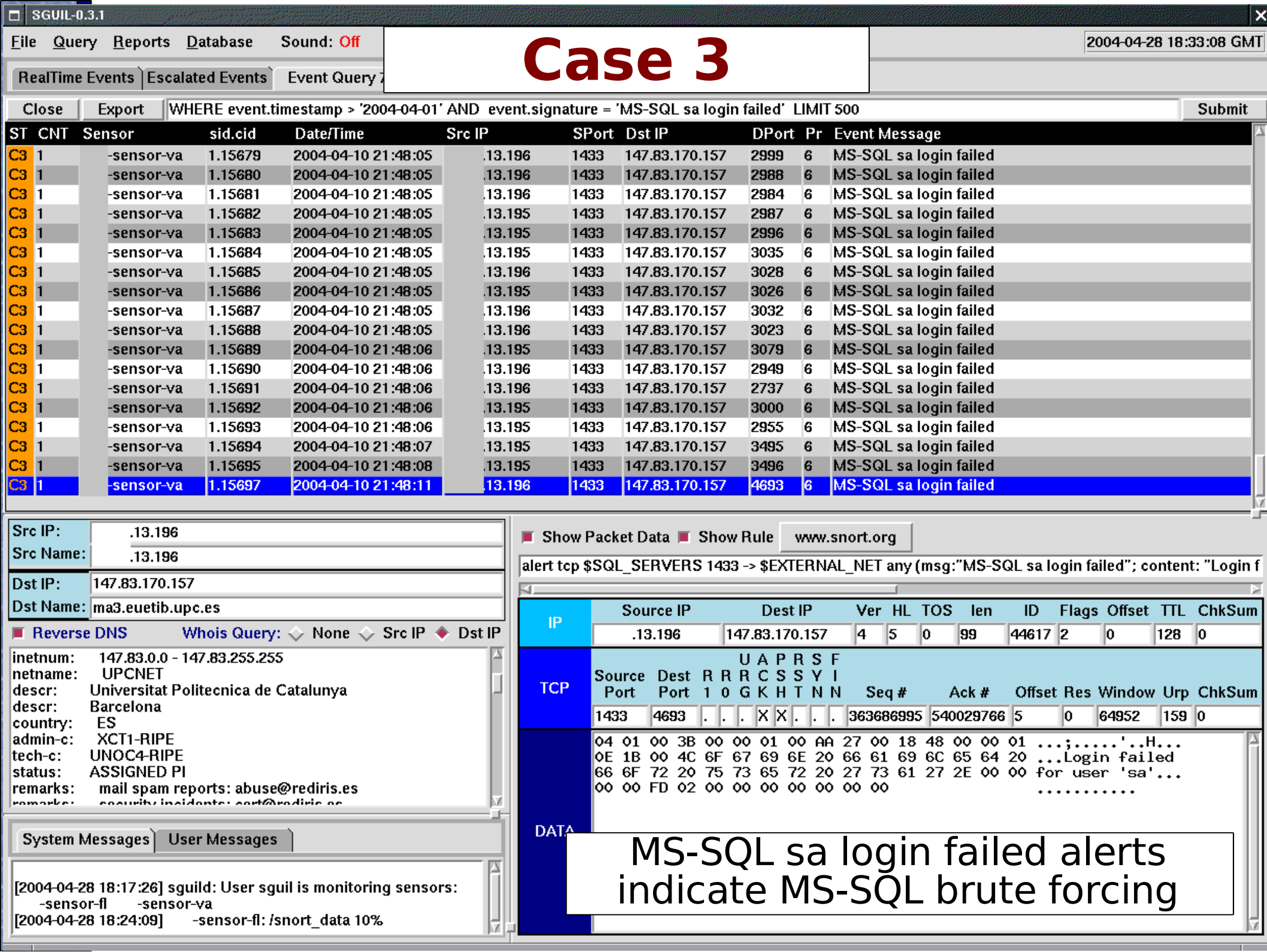


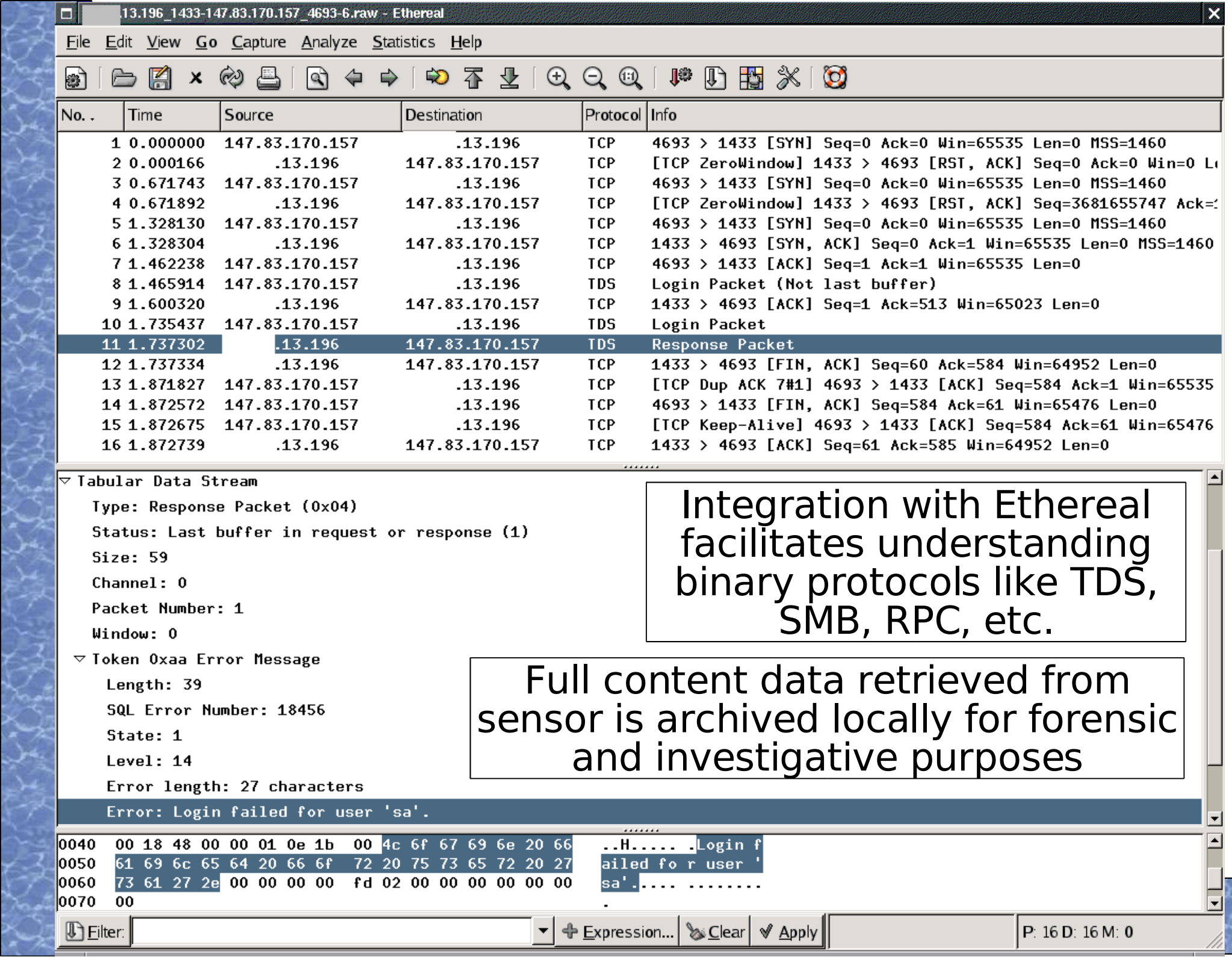

SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:54:24 GMT
Case 1
RealTime Events Escalated Events
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 2 -sensor-va 1.30963 2004-04-27 19:40:41 67.18.117.150 50361 .13.196 8080 6 SCAN Proxy Port 8080 attempt
RT 1 -sensor-va 1.30975 2004-04-27 20:14:05 67.234.73.61 0 .13.197 8080 6 SCAN Proxy Port 8080 attempt
RT 1 -sensor-va 1.30984 2004-04-27 20:54:10 13.201 80 67.166.22.213 1547 6 ATTACK-RESPONSES 403 Forbidden
RT 1 -sensor-va 1.30985 2004-04-27 20:58:07 67.234.73.173 0 .13.200 8080 6 SCAN Proxy Port 8080 attempt
RT 1 -sensor-va 1.31078 2004-04-27 22:31:16 67.234.73.190 0 .13.202 8080 6 SCAN Proxy Port 8080 attempt
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 10 -sensor-va 1.31468 2004-04-28 12:40:57 216.148.246.132 53 .13.194 0 17 BAD-TRAFFIC udp port 0 traffic
RT 5
RT 10
RT 10
RT 1
Why did the target respond with 403 Forbidden? This isn't very useful -- it's the intruder's attempt which is more important (even though it failed)
ST CN
RT 1
RT 1 -sensor-va 1.31652 2004-04-28 18:10:40 81.59.95.30 1689 13.199 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31655 2004-04-28 18:22:36 205.205.1.116 3766 13.198 21 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31659 2004-04-28 18:35:41 69.37.90.39 4499 13.198 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-fl 2.1390 2004-04-28 18:37:01 217.233.127.125 4066 .152.50 135 6 spp_portscan: Portscan Detected
Src IP: .13.201
Src Name: .13.201
Dst IP: 67.166.22.213
Dst Name: c-67-166-22-213.client.comcast.net
Reverse DNS Whois Query: None Src IP Dst IP
CustName: Comcast Cable Communications, IP Services
Address: 3 Executive Campus
Address: 5th Floor
City: Cherry Hill
StateProv: NJ
PostalCode: 08002
Country: US
RegDate: 2003-06-19
Updated: 2003-06-19
System Messages User Messages
-sensor-fl -sensor-va
[2004-04-28 18:24:09] -sensor-fl: /snort_data 10%
[2004-04-28 18:46:51] -sensor-va: /snort_data 80%
[2004-04-28 18:50:54] -sensor-fl: /snort_data 10%
Show Packet Data Show Rule www.snort.org
flow:from_server,established; content:"HTTP/1.1 403"; depth:12; classtype:attempted-recon; sid:1201; re
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
.13.201 67.166.22.213 4 5 0 245 26242 2 0 128 1
TCP Source Port Dest Port R R U A P R S F Seq # Ack # Offset Res Window Urp ChkSum
1 0 R C S H T N N
80 1547 . . . X X . . . 240608196 604533130 5 0 64849 383 0
DATA
48 54 54 50 2F 31 2E 31 20 34 30 33 20 46 6F 72 HTTP/1.1 403 For
62 69 64 64 65 6E 0D 0A 53 65 72 76 65 72 3A 20 bidden..Server:
4D 69 63 72 6F 73 6F 66 74 2D 49 49 53 2F 35 2E Microsoft-IIS/5.
30 0D 0A 44 61 74 65 3A 20 54 75 65 2C 20 32 37 0..Date: Tue, 27
20 41 70 72 20 32 30 30 34 20 32 30 3A 35 35 3A Apr 2004 20:55:
31 36 20 47 4D 54 0D 0A 43 6F 6E 6E 65 63 74 69 16 GMT..Connecti
6F 6E 3A 20 63 6C 6F 73 65 0D 0A 43 6F 6E 74 65 on: close..Conte
6E 74 2D 54 79 70 65 3A 20 74 65 78 74 2F 68 74 nt-Type: text/ht
6D 6C 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 ml..Content-Leng
74 68 3A 20 31 34 31 0D 0A 4D 53 2D 57 65 62 53 th: 141..MS-WebS
74 6F 72 61 67 65 3A 20 36 2E 30 2E 36 32 34 39 torage: 6.0.6249
0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A ..Cache-Control:
20 6E 6F 2D 63 61 63 68 65 0D 0A 0D 0A no-cache....

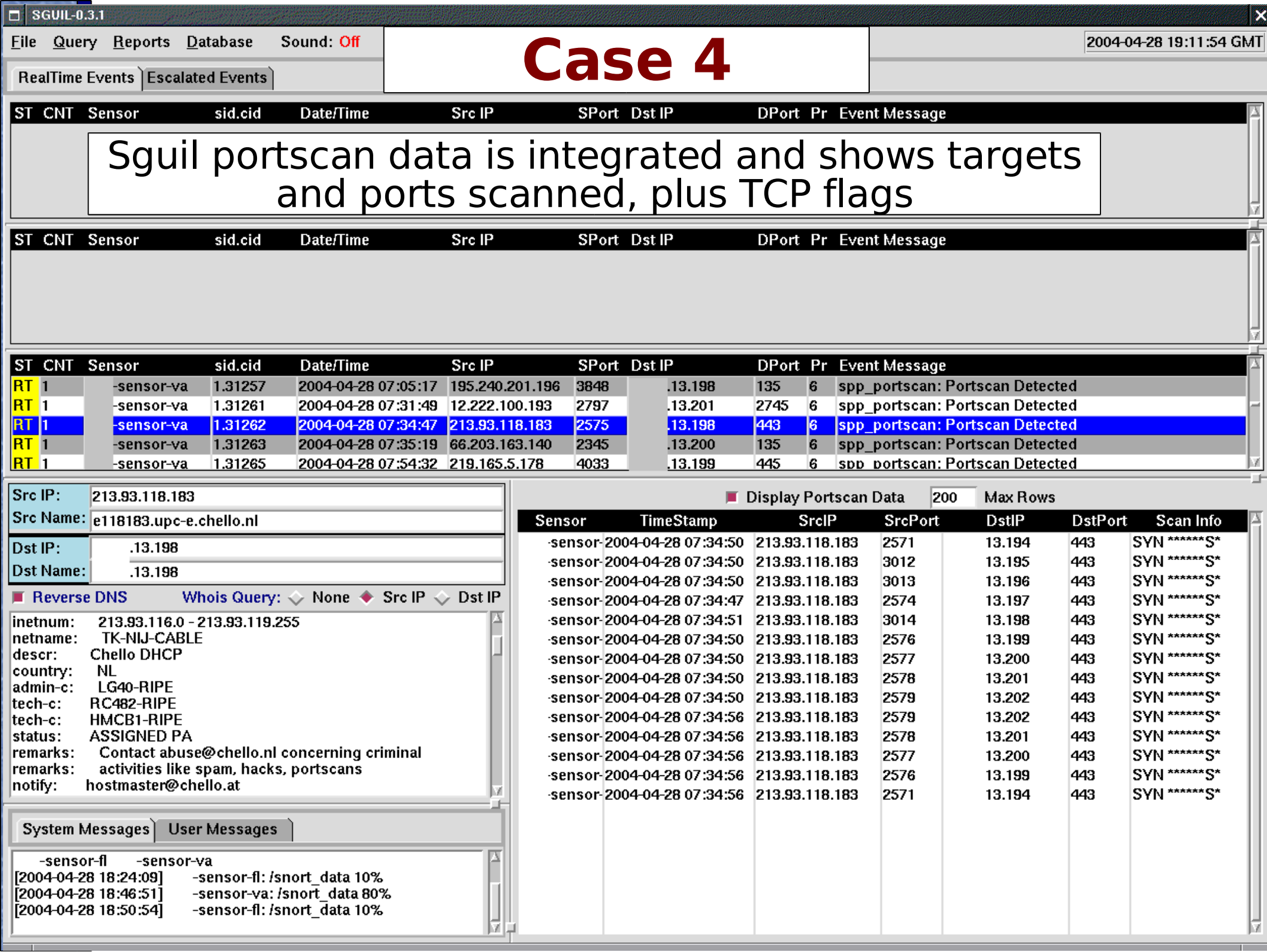
Transcript shows an attempted HTTP MOVE was not accepted by the server. This is not an attack.

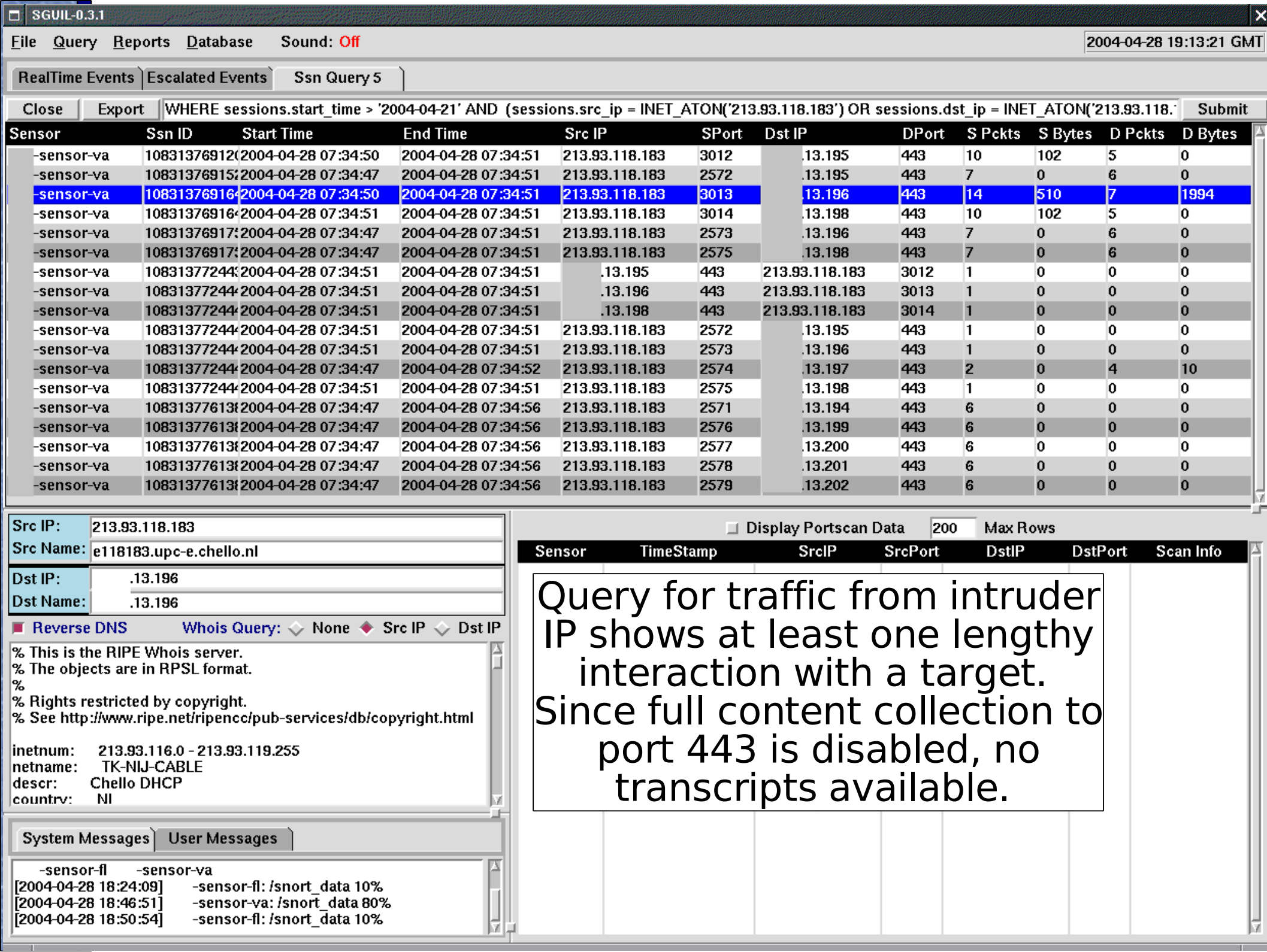

SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:40:17 GMT
Case 2
RealTime Events Escalated Events Event Qu
Close Export WHERE event.timestamp > '2004-04-01' AND event.status = 1 and event.signature like 'MS-SQL%' LIMIT 500 Submit
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
NA 1 sensor 1.344 2004-04-01 03:50:53 198.6.1.4 53 .153.34 1434 17 MS-SQL ping attempt
NA 1 sensor 1.7039 2004-04-05 17:54:14 198.6.1.5 53 .153.34 1434 17 MS-SQL ping attempt
NA 1 sensor 1.14957 2004-04-08 02:35:48 198.6.1.4 53 .153.34 1434 17 MS-SQL version overflow attempt
NA 1 sensor 1.27616 2004-04-17 10:42:44 198.6.1.4 53 .153.34 1434 17 MS-SQL ping attempt
NA 1 sensor 1.27653 2004-04-17 22:30:25 198.6.1.4 53 .153.34 1434 17 MS-SQL version overflow attempt
NA 1 sensor 1.28690 2004-04-22 22:26:17 198.6.1.4 53 .153.34 1434 17 MS-SQL ping attempt
NA 1 sensor 1.28691 2004-04-22 22:26:18 198.6.1.5 53 .153.34 1434 17 MS-SQL ping attempt
NA 1 sensor 1.28965 2004-04-24 16:54:41 198.6.1.3 53 .153.34 1434 17 MS-SQL version overflow attempt
MS-SQL version overflow attempt -- what caused this?
Src IP: 198.6.1.3
Src Name: cache02.ns.uu.net
Dst IP: .153.34
Dst Name: .com
Reverse DNS Whois Query: None Src IP Dst IP
OrgName: UUNET Technologies, Inc.
OrgID: UU
Address: 22001 Loudoun County Parkway
City: Ashburn
StateProv: VA
PostalCode: 20147
Country: US
System Messages User Messages
[2004-04-28 17:21:26] sensor: /snort_data 71%
[2004-04-28 17:51:26] sensor: /snort_data 71%
[2004-04-28 18:21:26] sensor: /snort_data 71%
Show Packet Data Show Rule www.snort.org
OME_NET 1434 (msg:"MS-SQL version overflow attempt"; content:"|04|"; offset:0; depth:1; dsize:>100;
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
198.6.1.3 .153.34 4 5 0 131 44134 2 0 246 0
UDP Port Port Length ChkSum
53 1434 111 47537
DATA
04 76 81 83 00 01 00 00 00 01 00 00 05 5F 6C 64 .v.....
61 70 04 5F 74 63 70 02 64 63 06 5F 6D 73 64 63 ap._tcp.dc._msdc
73 07 03 63 6F 6D 00 00 21 s. .com..!
00 01 C0 21 00 06 00 01 00 00 1B 02 00 29 05 6C ...!.....).l
65 77 69 73 C0 21 0A 70 6F 73 74 6D 61 73 74 65 ewis.!.postmaste
72 C0 21 77 73 42 3D 00 00 2A 30 00 00 0E 10 00 r.!wsB=..*0.....
09 3A 80 00 01 51 80 .:...Q.


198.6.1.3_53-[redacted].153.34_1434-17.raw - Ethereal
File Edit View Go Capture Analyze Statistics Help
No. . Time Source Destination Protocol Info
1 0.000000 [redacted].153.34 198.6.1.3 DNS Standard query SRV _ldap._tcp.dc._msdcs.[redacted].com
2 0.084216 198.6.1.3 .153.34 DNS Standard query response, No such name
Frame 1 (92 bytes on wire, 92 bytes captured)
Ethernet II, Src: 00:a0:cc:3d:77:c7, Dst: 00:30:19:1c:12:40
Internet Protocol, Src Addr: .153.34 (.153.34), Dst Addr: 198.6.1.3 (198.6.1.3)
User Datagram Protocol, Src Port: 1434 (1434), Dst Port: 53 (53)
Domain Name System (query)
Transaction ID: 0x0476
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
_ldap._tcp.dc._msdcs. .com: type SRV, class inet
Name: _ldap._tcp.dc._msdcs. .com
Type: Service location
Class: inet
Because we capture everything technically and legally possible, we see the outbound DNS query prompted a response which triggered Snort
0000 00 30 19 1c 12 40 00 a0 cc 3d 77 c7 08 00 45 00 .0...@.. .=w...E.
0010 00 4e e3 1b 00 00 7d 11 29 6c 99 22 c6 06 .N....}.)l..."..
0020 01 03 05 9a 00 35 00 3a fd d4 04 76 01 00 00 01 .....5.: ...v....
0030 00 00 00 00 00 00 05 5f 6c 64 61 70 04 5f 74 63 ...._ ldap._tc
0040 70 02 64 63 06 5f 6d 73 64 63 73 07 p.dc._ms dcs.
0050 03 63 6f 6d 00 00 21 00 01 .com. .!..
Filter: Expression... Clear Apply
P: 2 D: 2 M: 0


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:33:08 GMT
Case 3
RealTime Events Escalated Events Event Query 7
Close Export WHERE event.timestamp > '2004-04-01' AND event.signature = 'MS-SQL sa login failed' LIMIT 500 Submit
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
C3 1 -sensor-va 1.15679 2004-04-10 21:48:05 .13.196 1433 147.83.170.157 2999 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15680 2004-04-10 21:48:05 .13.196 1433 147.83.170.157 2988 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15681 2004-04-10 21:48:05 .13.196 1433 147.83.170.157 2984 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15682 2004-04-10 21:48:05 .13.195 1433 147.83.170.157 2987 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15683 2004-04-10 21:48:05 .13.195 1433 147.83.170.157 2996 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15684 2004-04-10 21:48:05 .13.195 1433 147.83.170.157 3035 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15685 2004-04-10 21:48:05 .13.196 1433 147.83.170.157 3028 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15686 2004-04-10 21:48:05 .13.195 1433 147.83.170.157 3026 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15687 2004-04-10 21:48:05 .13.196 1433 147.83.170.157 3032 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15688 2004-04-10 21:48:05 .13.196 1433 147.83.170.157 3023 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15689 2004-04-10 21:48:06 .13.195 1433 147.83.170.157 3079 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15690 2004-04-10 21:48:06 .13.196 1433 147.83.170.157 2949 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15691 2004-04-10 21:48:06 .13.196 1433 147.83.170.157 2737 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15692 2004-04-10 21:48:06 .13.195 1433 147.83.170.157 3000 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15693 2004-04-10 21:48:06 .13.195 1433 147.83.170.157 2955 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15694 2004-04-10 21:48:07 .13.195 1433 147.83.170.157 3495 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15695 2004-04-10 21:48:08 .13.195 1433 147.83.170.157 3496 6 MS-SQL sa login failed
C3 1 -sensor-va 1.15697 2004-04-10 21:48:11 .13.196 1433 147.83.170.157 4693 6 MS-SQL sa login failed
Src IP: .13.196
Src Name: .13.196
Dst IP: 147.83.170.157
Dst Name: ma3.euetib.upc.es
Reverse DNS Whois Query: None Src IP Dst IP
inetnum: 147.83.0.0 - 147.83.255.255
netname: UPCNET
descr: Universitat Politecnica de Catalunya
descr: Barcelona
country: ES
admin-c: XCT1-RIPE
tech-c: UNOC4-RIPE
status: ASSIGNED PI
remarks: mail spam reports: abuse@rediris.es
Show Packet Data Show Rule www.snort.org
alert tcp $SQL_SERVERS 1433 -> $EXTERNAL_NET any (msg:"MS-SQL sa login failed"; content: "Login f
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
.13.196 147.83.170.157 4 5 0 99 44617 2 0 128 0
TCP Source Port Dest Port R R U A P R S F Seq # Ack # Offset Res Window Urp ChkSum
1433 4693 . . . X X . . . 363686995 540029766 5 0 64952 159 0
DATA
04 01 00 3B 00 00 01 00 AA 27 00 18 48 00 00 01 ...;.....'..H...
0E 1B 00 4C 6F 67 69 6E 20 66 61 69 6C 65 64 20 ...Login failed
66 6F 72 20 75 73 65 72 20 27 73 61 27 2E 00 00 for user 'sa'...
00 00 FD 02 00 00 00 00 00 00 00 ....
System Messages User Messages
[2004-04-28 18:17:26] sguild: User sguil is monitoring sensors:
-sensor-fl -sensor-va
[2004-04-28 18:24:09] -sensor-fl: /snort_data 10%
MS-SQL sa login failed alerts indicate MS-SQL brute forcing


13.196_1433-147.83.170.157_4693-6.raw - Ethereal
File Edit View Go Capture Analyze Statistics Help
No. Time Source Destination Protocol Info
1 0.000000 147.83.170.157 .13.196 TCP 4693 > 1433 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
2 0.000166 .13.196 147.83.170.157 TCP [TCP ZeroWindow] 1433 > 4693 [RST, ACK] Seq=0 Ack=0 Win=0 L
3 0.671743 147.83.170.157 .13.196 TCP 4693 > 1433 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
4 0.671892 .13.196 147.83.170.157 TCP [TCP ZeroWindow] 1433 > 4693 [RST, ACK] Seq=3681655747 Ack=
5 1.328130 147.83.170.157 .13.196 TCP 4693 > 1433 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
6 1.328304 .13.196 147.83.170.157 TCP 1433 > 4693 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
7 1.462238 147.83.170.157 .13.196 TCP 4693 > 1433 [ACK] Seq=1 Ack=1 Win=65535 Len=0
8 1.465914 147.83.170.157 .13.196 TDS Login Packet (Not last buffer)
9 1.600320 .13.196 147.83.170.157 TCP 1433 > 4693 [ACK] Seq=1 Ack=513 Win=65023 Len=0
10 1.735437 147.83.170.157 .13.196 TDS Login Packet
11 1.737302 .13.196 147.83.170.157 TDS Response Packet
12 1.737334 .13.196 147.83.170.157 TCP 1433 > 4693 [FIN, ACK] Seq=60 Ack=584 Win=64952 Len=0
13 1.871827 147.83.170.157 .13.196 TCP [TCP Dup ACK 7#1] 4693 > 1433 [ACK] Seq=584 Ack=1 Win=65535
14 1.872572 147.83.170.157 .13.196 TCP 4693 > 1433 [FIN, ACK] Seq=584 Ack=61 Win=65476 Len=0
15 1.872675 147.83.170.157 .13.196 TCP [TCP Keep-Alive] 4693 > 1433 [ACK] Seq=584 Ack=61 Win=65476
16 1.872739 .13.196 147.83.170.157 TCP 1433 > 4693 [ACK] Seq=61 Ack=585 Win=64952 Len=0
Tabular Data Stream
Type: Response Packet (0x04)
Status: Last buffer in request or response (1)
Size: 59
Channel: 0
Packet Number: 1
Window: 0
Token 0xaa Error Message
Length: 39
SQL Error Number: 18456
State: 1
Level: 14
Error length: 27 characters
Error: Login failed for user 'sa'.
0040 00 18 48 00 00 01 0e 1b 00 4c 6f 67 69 6e 20 66 ..H..... .Login f
0050 61 69 6c 65 64 20 66 6f 72 20 75 73 65 72 20 27 ailed fo r user '
0060 73 61 27 2e 00 00 00 00 fd 02 00 00 00 00 00 00 sa'.... ....
0070 00 .
Filter: Expression... Clear Apply
P: 16 D: 16 M: 0
Integration with Ethereal facilitates understanding binary protocols like TDS, SMB, RPC, etc.
Full content data retrieved from sensor is archived locally for forensic and investigative purposes

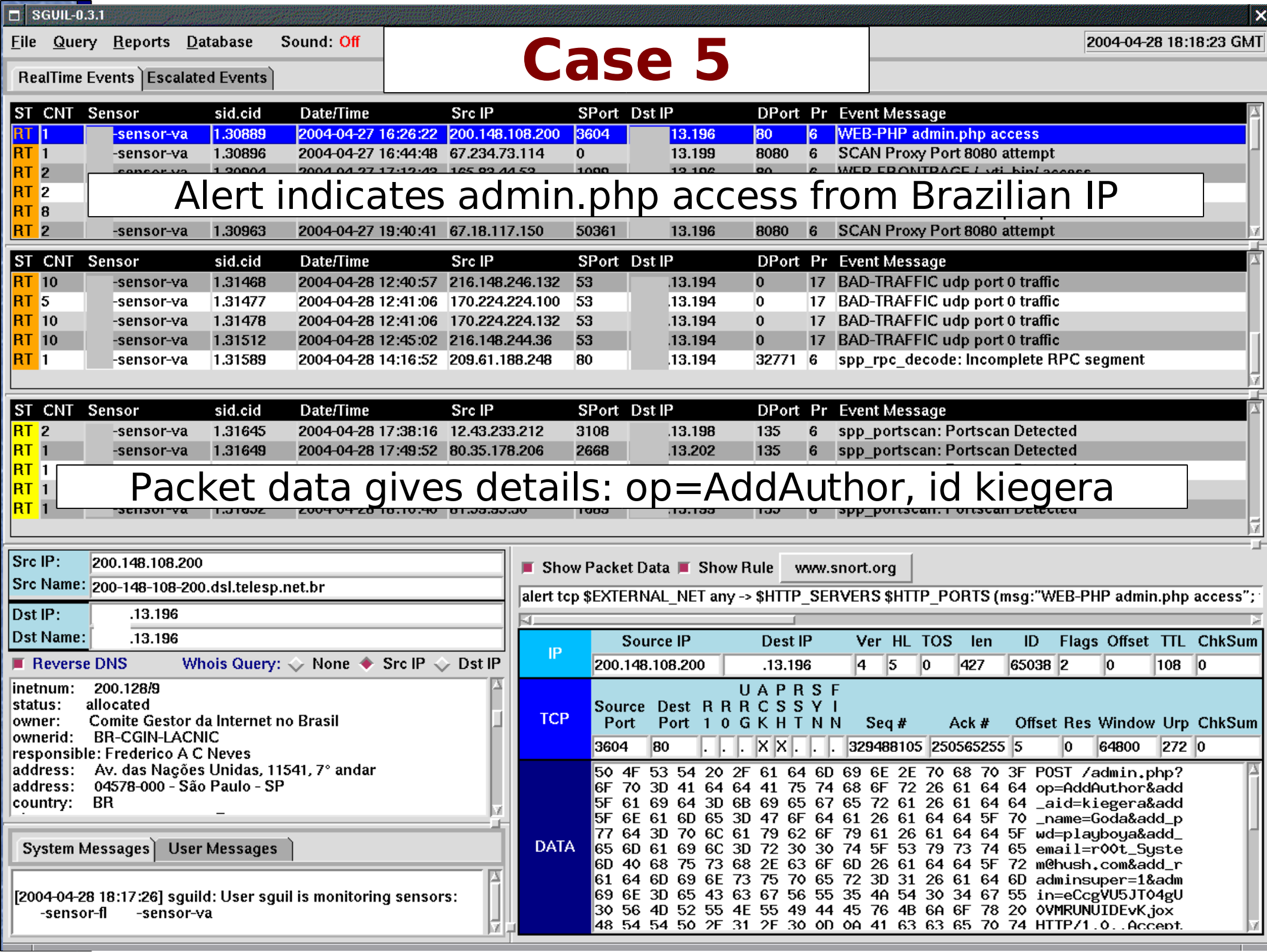

SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 19:11:54 GMT
Case 4
RealTime Events Escalated Events
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
Sguil portscan data is integrated and shows targets and ports scanned, plus TCP flags
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 -sensor-va 1.31257 2004-04-28 07:05:17 195.240.201.196 3848 .13.198 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31261 2004-04-28 07:31:49 12.222.100.193 2797 .13.201 2745 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31262 2004-04-28 07:34:47 213.93.118.183 2575 .13.198 443 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31263 2004-04-28 07:35:19 66.203.163.140 2345 .13.200 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31265 2004-04-28 07:54:32 219.165.5.178 4033 .13.199 445 6 spp_portscan: Portscan Detected
Src IP: 213.93.118.183
Src Name: e118183.upc-e.chello.nl
Dst IP: .13.198
Dst Name: .13.198
Reverse DNS Whois Query: None Src IP Dst IP
inetnum: 213.93.116.0 - 213.93.119.255
netname: TK-NIJ-CABLE
descr: Chello DHCP
country: NL
admin-c: LG40-RIPE
tech-c: RC482-RIPE
tech-c: HMCB1-RIPE
status: ASSIGNED PA
remarks: Contact abuse@chello.nl concerning criminal
remarks: activities like spam, hacks, portscans
notify: hostmaster@chello.at
System Messages User Messages
-sensor-fl -sensor-va
[2004-04-28 18:24:09] -sensor-fl: /snort_data 10%
[2004-04-28 18:46:51] -sensor-va: /snort_data 80%
[2004-04-28 18:50:54] -sensor-fl: /snort_data 10%
Display Portscan Data 200 Max Rows
Sensor TimeStamp SrcIP SrcPort DstIP DstPort Scan Info
-sensor- 2004-04-28 07:34:50 213.93.118.183 2571 13.194 443 SYN ******S*
-sensor- 2004-04-28 07:34:50 213.93.118.183 3012 13.195 443 SYN ******S*
-sensor- 2004-04-28 07:34:50 213.93.118.183 3013 13.196 443 SYN ******S*
-sensor- 2004-04-28 07:34:47 213.93.118.183 2574 13.197 443 SYN ******S*
-sensor- 2004-04-28 07:34:51 213.93.118.183 3014 13.198 443 SYN ******S*
-sensor- 2004-04-28 07:34:50 213.93.118.183 2576 13.199 443 SYN ******S*
-sensor- 2004-04-28 07:34:50 213.93.118.183 2577 13.200 443 SYN ******S*
-sensor- 2004-04-28 07:34:50 213.93.118.183 2578 13.201 443 SYN ******S*
-sensor- 2004-04-28 07:34:50 213.93.118.183 2579 13.202 443 SYN ******S*
-sensor- 2004-04-28 07:34:56 213.93.118.183 2579 13.202 443 SYN ******S*
-sensor- 2004-04-28 07:34:56 213.93.118.183 2578 13.201 443 SYN ******S*
-sensor- 2004-04-28 07:34:56 213.93.118.183 2577 13.200 443 SYN ******S*
-sensor- 2004-04-28 07:34:56 213.93.118.183 2576 13.199 443 SYN ******S*
-sensor- 2004-04-28 07:34:56 213.93.118.183 2571 13.194 443 SYN ******S*


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 19:13:21 GMT
RealTime Events Escalated Events Ssn Query 5
Close Export
WHERE sessions.start_time > '2004-04-21' AND (sessions.src_ip = INET_ATON('213.93.118.183') OR sessions.dst_ip = INET_ATON('213.93.118.
Submit
Sensor Ssn ID Start Time End Time Src IP SPort Dst IP DPort S Pckts S Bytes D Pckts D Bytes
-sensor-va 10831376912 2004-04-28 07:34:50 2004-04-28 07:34:51 213.93.118.183 3012 .13.195 443 10 102 5 0
-sensor-va 10831376915 2004-04-28 07:34:47 2004-04-28 07:34:51 213.93.118.183 2572 .13.195 443 7 0 6 0
-sensor-va 10831376916 2004-04-28 07:34:50 2004-04-28 07:34:51 213.93.118.183 3013 .13.196 443 14 510 7 1994
-sensor-va 10831376916 2004-04-28 07:34:51 2004-04-28 07:34:51 213.93.118.183 3014 .13.198 443 10 102 5 0
-sensor-va 10831376917 2004-04-28 07:34:47 2004-04-28 07:34:51 213.93.118.183 2573 .13.196 443 7 0 6 0
-sensor-va 10831376917 2004-04-28 07:34:47 2004-04-28 07:34:51 213.93.118.183 2575 .13.198 443 7 0 6 0
-sensor-va 10831377244 2004-04-28 07:34:51 2004-04-28 07:34:51 .13.195 443 213.93.118.183 3012 1 0 0 0
-sensor-va 10831377244 2004-04-28 07:34:51 2004-04-28 07:34:51 .13.196 443 213.93.118.183 3013 1 0 0 0
-sensor-va 10831377244 2004-04-28 07:34:51 2004-04-28 07:34:51 .13.198 443 213.93.118.183 3014 1 0 0 0
-sensor-va 10831377244 2004-04-28 07:34:51 2004-04-28 07:34:51 213.93.118.183 2572 .13.195 443 1 0 0 0
-sensor-va 10831377244 2004-04-28 07:34:51 2004-04-28 07:34:51 213.93.118.183 2573 .13.196 443 1 0 0 0
-sensor-va 10831377244 2004-04-28 07:34:47 2004-04-28 07:34:52 213.93.118.183 2574 .13.197 443 2 0 4 10
-sensor-va 10831377244 2004-04-28 07:34:51 2004-04-28 07:34:51 213.93.118.183 2575 .13.198 443 1 0 0 0
-sensor-va 10831377613 2004-04-28 07:34:47 2004-04-28 07:34:56 213.93.118.183 2571 .13.194 443 6 0 0 0
-sensor-va 10831377613 2004-04-28 07:34:47 2004-04-28 07:34:56 213.93.118.183 2576 .13.199 443 6 0 0 0
-sensor-va 10831377613 2004-04-28 07:34:47 2004-04-28 07:34:56 213.93.118.183 2577 .13.200 443 6 0 0 0
-sensor-va 10831377613 2004-04-28 07:34:47 2004-04-28 07:34:56 213.93.118.183 2578 .13.201 443 6 0 0 0
-sensor-va 10831377613 2004-04-28 07:34:47 2004-04-28 07:34:56 213.93.118.183 2579 .13.202 443 6 0 0 0
Src IP: 213.93.118.183
Src Name: e118183.upc-e.chello.nl
Dst IP: .13.196
Dst Name: .13.196
Reverse DNS Whois Query: None Src IP Dst IP
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html
inetnum: 213.93.116.0 - 213.93.119.255
netname: TK-NIJ-CABLE
descr: Chello DHCP
country: NL
Display Portscan Data 200 Max Rows
Sensor TimeStamp SrcIP SrcPort DstIP DstPort Scan Info
Query for traffic from intruder IP shows at least one lengthy interaction with a target. Since full content collection to port 443 is disabled, no transcripts available.
System Messages User Messages
-sensor-fl -sensor-va
[2004-04-28 18:24:09] -sensor-fl: /snort_data 10%
[2004-04-28 18:46:51] -sensor-va: /snort_data 80%
[2004-04-28 18:50:54] -sensor-fl: /snort_data 10%

Still query for session data around the time of the attack to see if target system suddenly initiated an outbound connection, or if a new party connected to the victim on another port. Essentially, look for anything suspicious. Nothing happened here, so our estimate is all is well.

Close | Export | WHERE sessions.start_time between '2004-04-28 07:34' and '2004-04-28 07:40' AND (sessions.src_ip = INET_ATON(' .13.196') OR sessic | Submit

Sensor	Ssn ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes
-sensor-va	10831376923	2004-04-28 07:34:00	2004-04-28 07:34:00	216.99.65.10	40480	.13.196	443	12	1404	8	612
-sensor-va	1083137646(	2004-04-28 07:34:05	2004-04-28 07:34:06	164.159.185.74	4671	.13.196	443	3	0	4	0
-sensor-va	1083137646(	2004-04-28 07:34:05	2004-04-28 07:34:06	164.159.185.74	4672	.13.196	443	3	0	4	0
-sensor-va	10831376923	2004-04-28 07:34:05	2004-04-28 07:34:06	164.159.185.74	4673	.13.196	443	16	2532	12	3200
-sensor-va	10831376923	2004-04-28 07:34:06	2004-04-28 07:34:06	164.159.185.74	4671	.13.196	443	1	0	0	0
-sensor-va	10831376923	2004-04-28 07:34:06	2004-04-28 07:34:06	164.159.185.74	4672	.13.196	443	1	0	0	0
-sensor-va	10831376923	2004-04-28 07:34:06	2004-04-28 07:34:07	164.159.185.74	4674	.13.196	443	12	1340	8	612
-sensor-va	10831376817	2004-04-28 07:34:41	2004-04-28 07:34:41	165.83.9.71	3505	.13.196	443	3	0	4	0
-sensor-va	10831376817	2004-04-28 07:34:41	2004-04-28 07:34:41	165.83.9.71	3506	.13.196	443	3	0	4	0
-sensor-va	1083137724(	2004-04-28 07:34:41	2004-04-28 07:34:41	165.83.9.71	3505	.13.196	443	1	0	0	0
-sensor-va	1083137724(	2004-04-28 07:34:41	2004-04-28 07:34:41	165.83.9.71	3506	.13.196	443	1	0	0	0
-sensor-va	1083137724(	2004-04-28 07:34:41	2004-04-28 07:34:43	165.83.9.71	3509	.13.196	443	16	2620	12	5128
-sensor-va	1083137724(	2004-04-28 07:34:43	2004-04-28 07:34:44	165.83.9.71	3510	.13.196	443	12	1302	8	612
-sensor-va	10831376917	2004-04-28 07:34:47	2004-04-28 07:34:51	213.93.118.183	2573	.13.196	443	7	0	6	0
-sensor-va	10831376916	2004-04-28 07:34:50	2004-04-28 07:34:51	213.93.118.183	3013	.13.196	443	14	510	7	1994
-sensor-va	1083137724(	2004-04-28 07:34:51	2004-04-28 07:34:51	.13.196	443	213.93.118.183	3013	1	0	0	0
-sensor-va	1083137724(	2004-04-28 07:34:51	2004-04-28 07:34:51	213.93.118.183	2573	.13.196	443	1	0	0	0
-sensor-va	10831377007	2004-04-28 07:35:00	2004-04-28 07:35:00	216.99.65.10	40477	.13.196	443	3	0	4	0
-sensor-va	10831377007	2004-04-28 07:35:00	2004-04-28 07:35:00	216.99.65.10	40480	.13.196	443	3	0	4	0
-sensor-va	10831377613	2004-04-28 07:35:00	2004-04-28 07:35:00	216.99.65.10	40477	.13.196	443	1	0	0	0
-sensor-va	10831377613	2004-04-28 07:35:00	2004-04-28 07:35:00	216.99.65.10	40480	.13.196	443	1	0	0	0
-sensor-va	1083137761(	2004-04-28 07:35:00	2004-04-28 07:36:01	216.99.65.10	40675	.13.196	443	19	2666	16	3200
-sensor-va	10831377613	2004-04-28 07:35:01	2004-04-28 07:35:01	216.99.65.10	40677	.13.196	443	12	1404	8	612
-sensor-va	1083137707(	2004-04-28 07:35:06	2004-04-28 07:35:07	164.159.185.74	4674	.13.196	443	3	0	4	0
-sensor-va	10831377613	2004-04-28 07:35:06	2004-04-28 07:35:07	164.159.185.74	4675	.13.196	443	16	2532	12	3200
-sensor-va	10831377613	2004-04-28 07:35:07	2004-04-28 07:35:07	164.159.185.74	4674	.13.196	443	1	0	0	0
-sensor-va	10831377613	2004-04-28 07:35:07	2004-04-28 07:35:08	164.159.185.74	4676	.13.196	443	12	1340	8	612
-sensor-va	10831377087	2004-04-28 07:35:08	2004-04-28 07:35:08	164.159.185.74	4673	.13.196	443	3	0	4	0
-sensor-va	10831377613	2004-04-28 07:35:08	2004-04-28 07:35:08	164.159.185.74	4673	.13.196	443	1	0	0	0
-sensor-va	10831377167	2004-04-28 07:35:16	2004-04-28 07:35:16	24.210.223.71	2781	.13.196	443	3	0	4	0


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:18:23 GMT
Case 5
RealTime Events Escalated Events
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 -sensor-va 1.30889 2004-04-27 16:26:22 200.148.108.200 3604 13.196 80 6 WEB-PHP admin.php access
RT 1 -sensor-va 1.30896 2004-04-27 16:44:48 67.234.73.114 0 13.199 8080 6 SCAN Proxy Port 8080 attempt
RT 2
RT 2
RT 8
RT 2 -sensor-va 1.30963 2004-04-27 19:40:41 67.18.117.150 50361 13.196 8080 6 SCAN Proxy Port 8080 attempt
Alert indicates admin.php access from Brazilian IP
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 10 -sensor-va 1.31468 2004-04-28 12:40:57 216.148.246.132 53 .13.194 0 17 BAD-TRAFFIC udp port 0 traffic
RT 5 -sensor-va 1.31477 2004-04-28 12:41:06 170.224.224.100 53 .13.194 0 17 BAD-TRAFFIC udp port 0 traffic
RT 10 -sensor-va 1.31478 2004-04-28 12:41:06 170.224.224.132 53 .13.194 0 17 BAD-TRAFFIC udp port 0 traffic
RT 10 -sensor-va 1.31512 2004-04-28 12:45:02 216.148.244.36 53 .13.194 0 17 BAD-TRAFFIC udp port 0 traffic
RT 1 -sensor-va 1.31589 2004-04-28 14:16:52 209.61.188.248 80 .13.194 32771 6 spp_rpc_decode: Incomplete RPC segment
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 2 -sensor-va 1.31645 2004-04-28 17:38:16 12.43.233.212 3108 .13.198 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.31649 2004-04-28 17:49:52 80.35.178.206 2668 .13.202 135 6 spp_portscan: Portscan Detected
RT 1
RT 1
RT 1
Packet data gives details: op=AddAuthor, id kiegera
Src IP: 200.148.108.200
Src Name: 200-148-108-200.dsl.telesp.net.br
Dst IP: .13.196
Dst Name: .13.196
Reverse DNS Whois Query: None Src IP Dst IP
inetnum: 200.128/9
status: allocated
owner: Comite Gestor da Internet no Brasil
ownerid: BR-CGIN-LACNIC
responsible: Frederico A C Neves
address: Av. das Nações Unidas, 11541, 7° andar
address: 04578-000 - São Paulo - SP
country: BR
System Messages User Messages
[2004-04-28 18:17:26] sguild: User sguil is monitoring sensors:
-sensor-fl -sensor-va
Show Packet Data Show Rule www.snort.org
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-PHP admin.php access";
IP
Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
200.148.108.200 .13.196 4 5 0 427 65038 2 0 108 0
TCP
Source Port Dest Port R R U A P R S F 1 0 R G K H T N N Seq # Ack # Offset Res Window Urp ChkSum
3604 80 . . . X X . . . 329488105 250565255 5 0 64800 272 0
DATA
50 4F 53 54 20 2F 61 64 6D 69 6E 2E 70 68 70 3F POST /admin.php?
6F 70 3D 41 64 64 41 75 74 68 6F 72 26 61 64 64 op=AddAuthor&add
5F 61 69 64 3D 6B 69 65 67 65 72 61 26 61 64 64 _aid=kiegera&add
5F 6E 61 6D 65 3D 47 6F 64 61 26 61 64 64 5F 70 _name=Goda&add_p
77 64 3D 70 6C 61 79 62 6F 79 61 26 61 64 64 5F wd=playboya&add_
65 6D 61 69 6C 3D 72 30 30 74 5F 53 79 73 74 65 email=r00t_Syste
6D 40 68 75 73 68 2E 63 6F 6D 26 61 64 64 5F 72 m@hush.com&add_r
61 64 6D 69 6E 73 75 70 65 72 3D 31 26 61 64 6D adminsuper=1&adm
69 6E 3D 65 43 63 67 56 55 35 4A 54 30 34 67 55 in=eCcgVU5JT04gU
30 56 4D 52 55 4E 55 49 44 45 76 4B 6A 6F 78 20 0VMRUNUIDEvKjox
48 54 54 50 2F 31 2F 30 0D 0A 41 63 63 65 70 74 HTTP/1.0..Accept

Transcript captures Web server reply showing 405 error

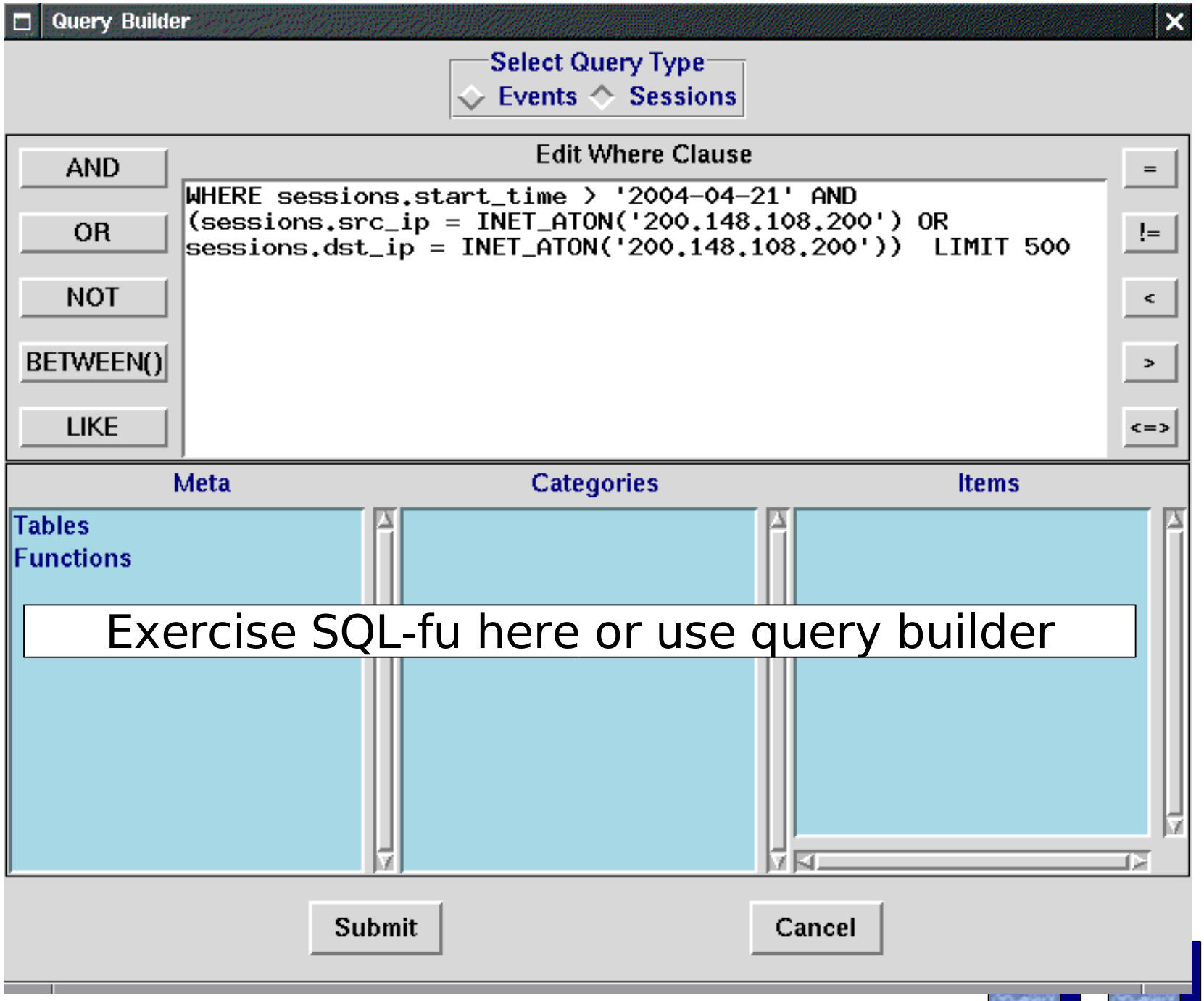
-sensor-va_30889

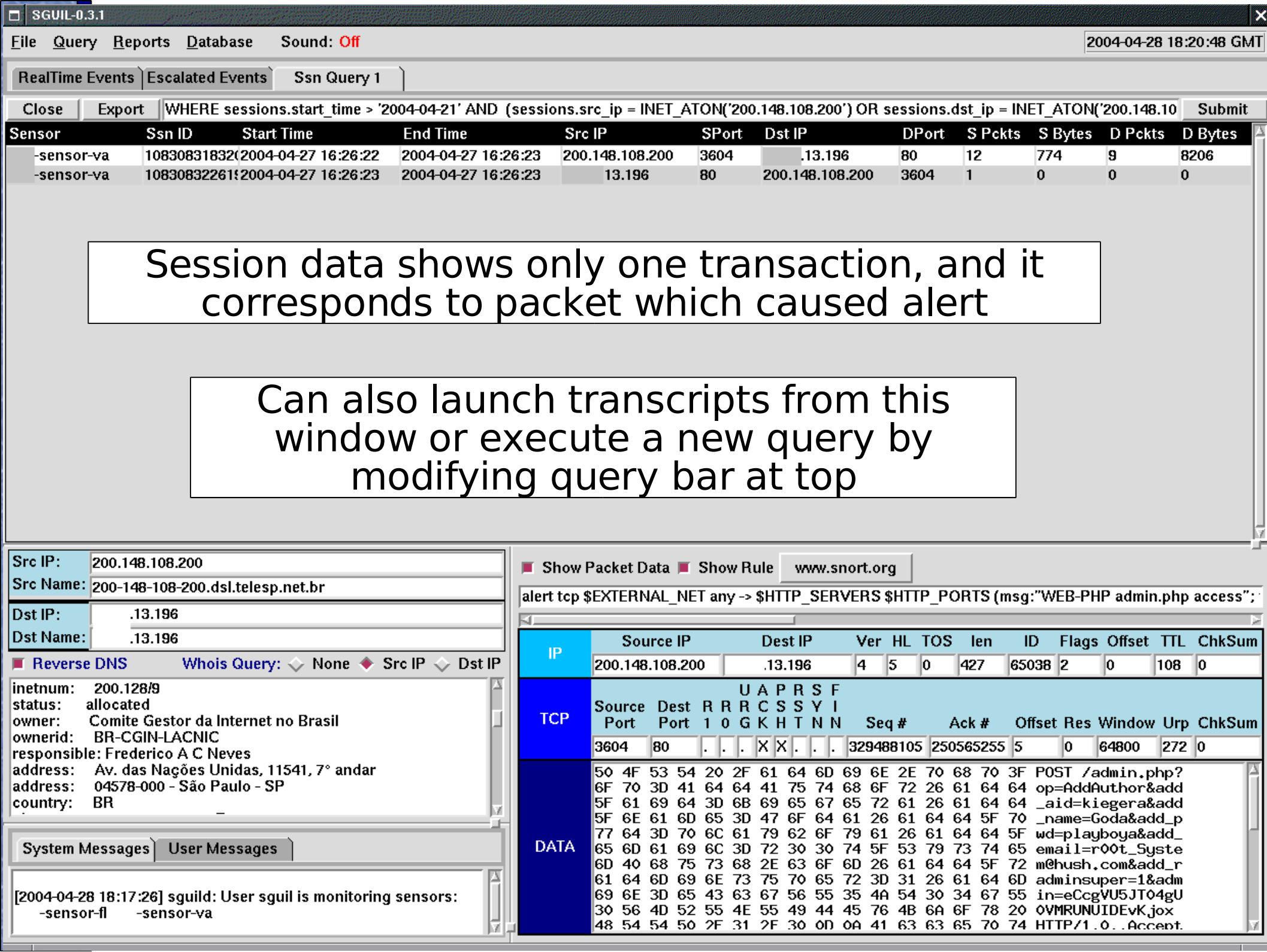
```
Sensor Name:        -sensor-va
Timestamp:          2004-04-27 16:26:22
Connection ID:      -sensor-va_30889
Src IP:             200.148.108.200    (200-148-108-200.dsl.telesp.net.br)
Dst IP:                .13.196         (        13.196)
Src Port:           3604
Dst Port:           80
=================================================================================
SRC: POST
/admin.php?op=AddAuthor&add_aid=kiegera&add_name=Goda&add_pwd=playboya&add_email=
r00t_System@hush.com&add_radminsuper=1&admin=eCcgVU5JT04gU0VMRUNUIDEvKjox
HTTP/1.0
SRC: Accept: */*
SRC: Accept-Language: en-us
SRC: Content-Encoding: gzip, deflate
SRC: Content-Type: application/x-www-form-urlencoded
SRC: Host:                      com
SRC: User-Agent: Mozilla 4.0 (Linux)
SRC: Content-Length:0
SRC: Connection: Close
SRC:
SRC:
DST: HTTP/1.1 405 Method not allowed
DST: Server: Microsoft-IIS/5.0
DST: Date: Tue, 27 Apr 2004 16:35:51 GMT
DST: Allow: OPTIONS, TRACE, GET, HEAD
DST: Content-Length: 3923
DST: Content-Type: text/html
DST:
```

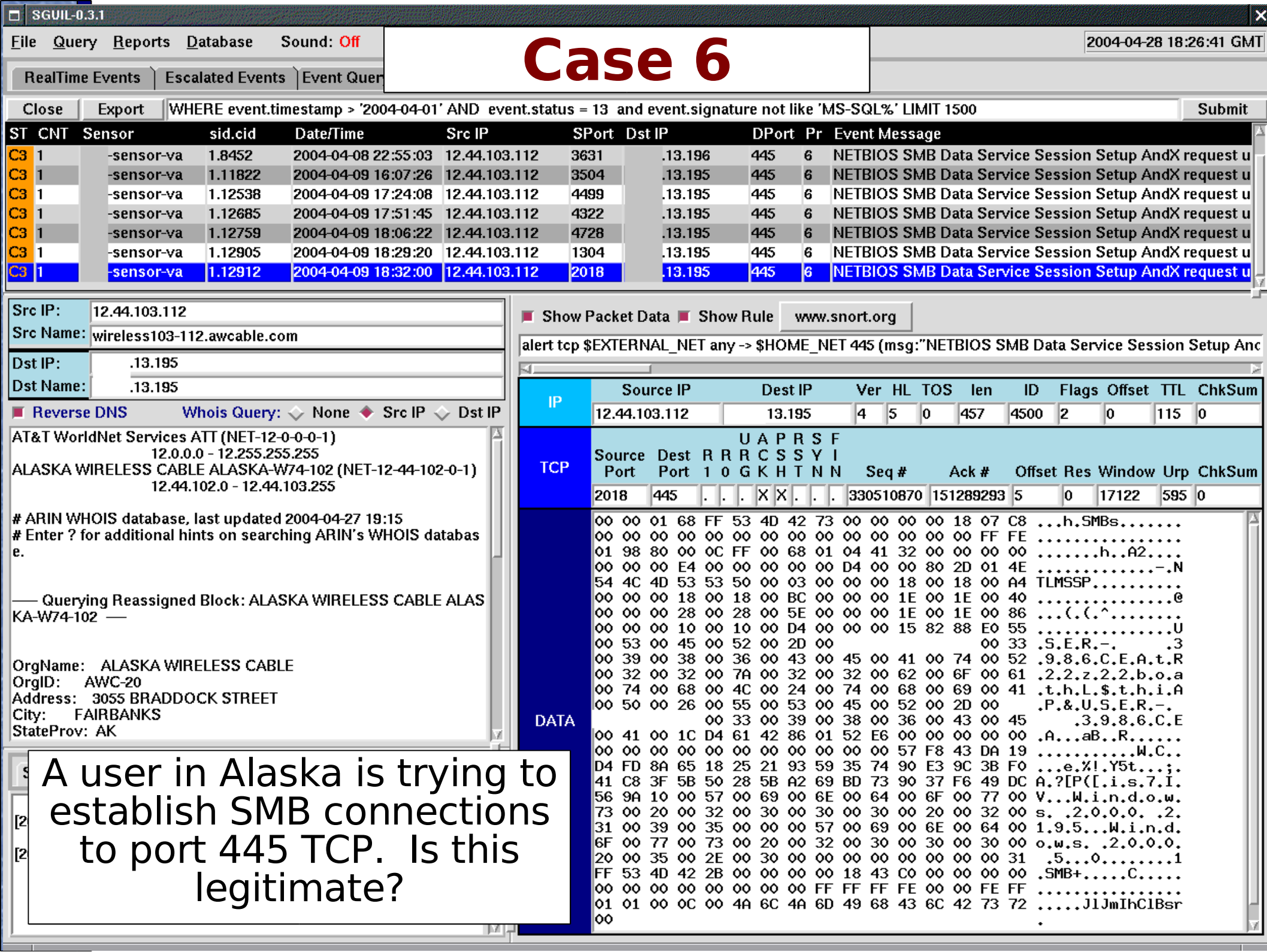
Debug Messages

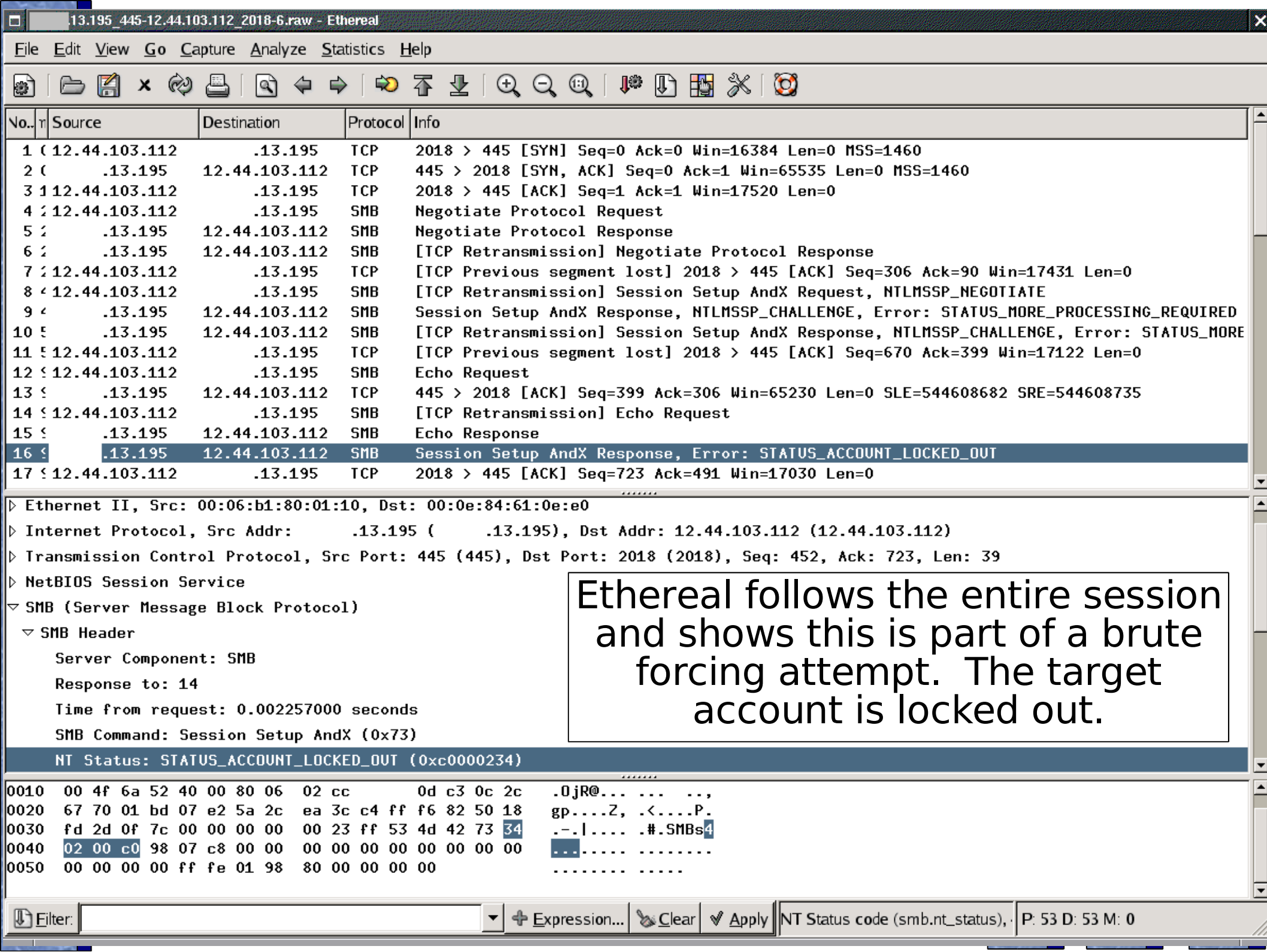
```
Your request has been sent to the server.
Please be patient as this can take some time.
Using archived data:
/snort_data/archive/2004-04-27/    -sensor-va/200.148.108.200:3604_      .13.196:80-6.raw
```

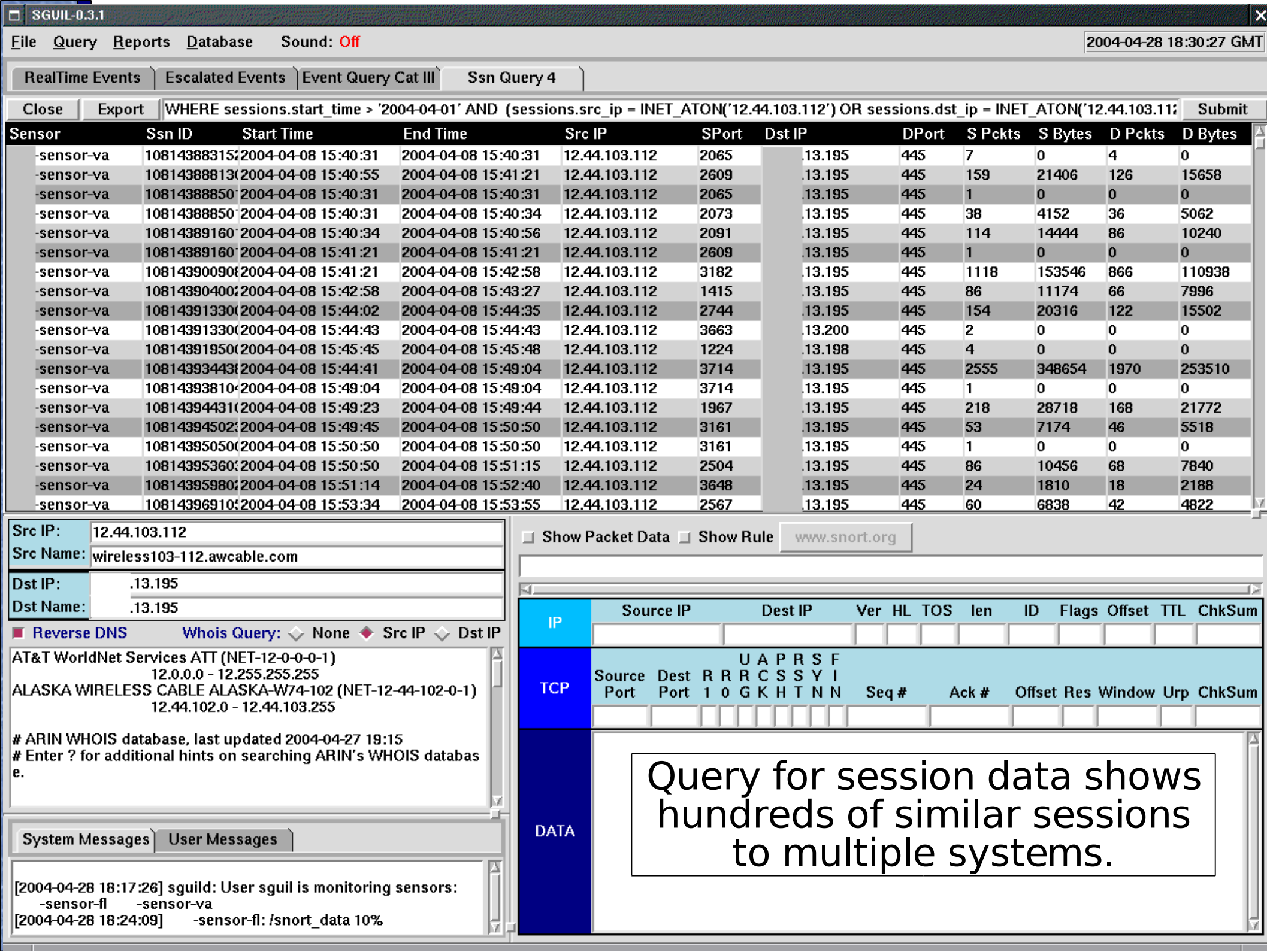
Did intruder do anything else? Query session data.

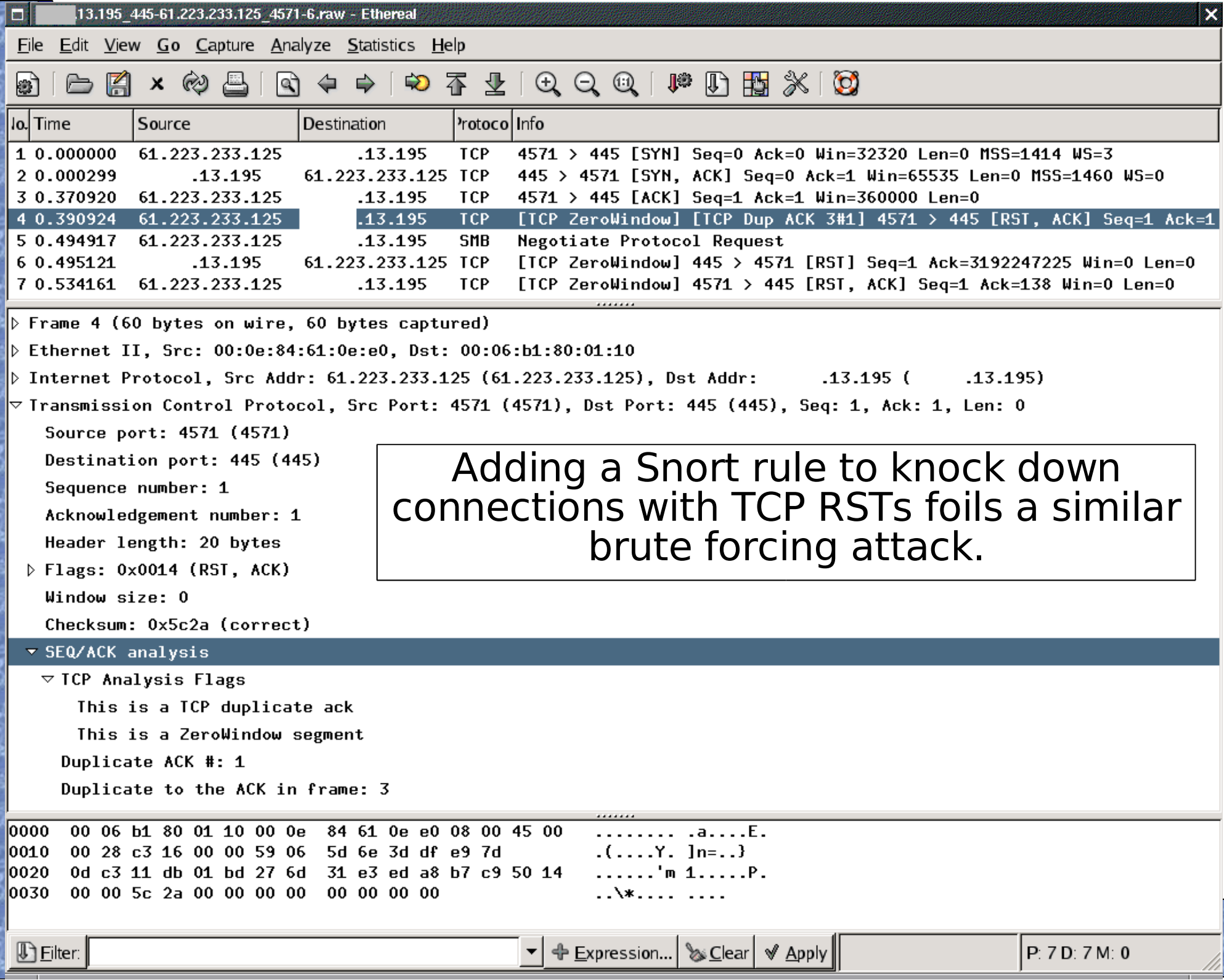



SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:20:48 GMT
RealTime Events Escalated Events Ssn Query 1
Close Export
WHERE sessions.start_time > '2004-04-21' AND (sessions.src_ip = INET_ATON('200.148.108.200') OR sessions.dst_ip = INET_ATON('200.148.10
Submit
Sensor Ssn ID Start Time End Time Src IP SPort Dst IP DPort S Pckts S Bytes D Pckts D Bytes
-sensor-va 10830831832 2004-04-27 16:26:22 2004-04-27 16:26:23 200.148.108.200 3604 .13.196 80 12 774 9 8206
-sensor-va 10830832261 2004-04-27 16:26:23 2004-04-27 16:26:23 13.196 80 200.148.108.200 3604 1 0 0 0
Session data shows only one transaction, and it corresponds to packet which caused alert
Can also launch transcripts from this window or execute a new query by modifying query bar at top
Src IP: 200.148.108.200
Src Name: 200-148-108-200.dsl.telesp.net.br
Dst IP: .13.196
Dst Name: .13.196
Reverse DNS Whois Query: None Src IP Dst IP
inetnum: 200.128/9
status: allocated
owner: Comite Gestor da Internet no Brasil
ownerid: BR-CGIN-LACNIC
responsible: Frederico A C Neves
address: Av. das Nações Unidas, 11541, 7° andar
address: 04578-000 - São Paulo - SP
country: BR
System Messages User Messages
[2004-04-28 18:17:26] sguild: User sguil is monitoring sensors:
-sensor-fl -sensor-va
Show Packet Data Show Rule www.snort.org
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-PHP admin.php access";
IP
Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
200.148.108.200 .13.196 4 5 0 427 65038 2 0 108 0
TCP
Source Port Dest Port R1 R0 URG ACK PSH RST SYN FIN Seq # Ack # Offset Res Window Urp ChkSum
3604 80 . . . X X . . . 329488105 250565255 5 0 64800 272 0
DATA
50 4F 53 54 20 2F 61 64 6D 69 6E 2E 70 68 70 3F POST /admin.php?
6F 70 3D 41 64 64 41 75 74 68 6F 72 26 61 64 64 op=AddAuthor&add
5F 61 69 64 3D 6B 69 65 67 65 72 61 26 61 64 64 _aid=kiegera&add
5F 6E 61 6D 65 3D 47 6F 64 61 26 61 64 64 5F 70 _name=Goda&add_p
77 64 3D 70 6C 61 79 62 6F 79 61 26 61 64 64 5F wd=playboya&add_
65 6D 61 69 6C 3D 72 30 30 74 5F 53 79 73 74 65 email=r00t_Syste
6D 40 68 75 73 68 2E 63 6F 6D 26 61 64 64 5F 72 m@hush.com&add_r
61 64 6D 69 6E 73 75 70 65 72 3D 31 26 61 64 6D adminsuper=1&adm
69 6E 3D 65 43 63 67 56 55 35 4A 54 30 34 67 55 in=eCcgVU5JT04gU
30 56 4D 52 55 4E 55 49 44 45 76 4B 6A 6F 78 20 0VMRUNUIDEvKjox
48 54 54 50 2F 31 2F 30 0D 0A 41 63 63 65 70 74 HTTP/1.0..Accept

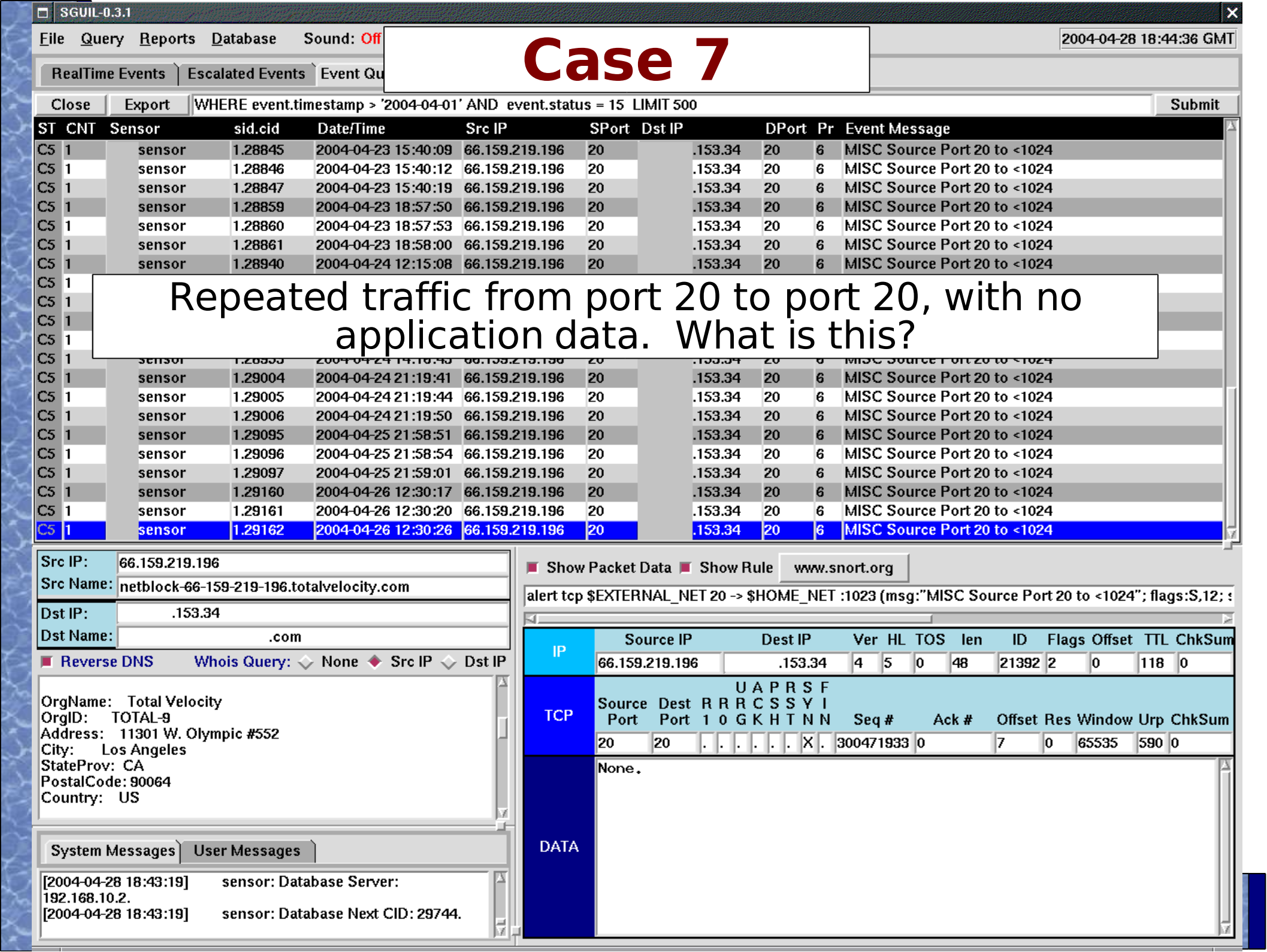

SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:26:41 GMT
Case 6
RealTime Events Escalated Events Event Quer
Close Export
WHERE event.timestamp > '2004-04-01' AND event.status = 13 and event.signature not like 'MS-SQL%' LIMIT 1500
Submit
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
C3 1 -sensor-va 1.8452 2004-04-08 22:55:03 12.44.103.112 3631 .13.196 445 6 NETBIOS SMB Data Service Session Setup AndX request u
C3 1 -sensor-va 1.11822 2004-04-09 16:07:26 12.44.103.112 3504 .13.195 445 6 NETBIOS SMB Data Service Session Setup AndX request u
C3 1 -sensor-va 1.12538 2004-04-09 17:24:08 12.44.103.112 4499 .13.195 445 6 NETBIOS SMB Data Service Session Setup AndX request u
C3 1 -sensor-va 1.12685 2004-04-09 17:51:45 12.44.103.112 4322 .13.195 445 6 NETBIOS SMB Data Service Session Setup AndX request u
C3 1 -sensor-va 1.12759 2004-04-09 18:06:22 12.44.103.112 4728 .13.195 445 6 NETBIOS SMB Data Service Session Setup AndX request u
C3 1 -sensor-va 1.12905 2004-04-09 18:29:20 12.44.103.112 1304 .13.195 445 6 NETBIOS SMB Data Service Session Setup AndX request u
C3 1 -sensor-va 1.12912 2004-04-09 18:32:00 12.44.103.112 2018 .13.195 445 6 NETBIOS SMB Data Service Session Setup AndX request u
Src IP: 12.44.103.112
Src Name: wireless103-112.awcable.com
Dst IP: .13.195
Dst Name: .13.195
Reverse DNS Whois Query: None Src IP Dst IP
AT&T WorldNet Services ATT (NET-12-0-0-0-1)
12.0.0.0 - 12.255.255.255
ALASKA WIRELESS CABLE ALASKA-W74-102 (NET-12-44-102-0-1)
12.44.102.0 - 12.44.103.255
ARIN WHOIS database, last updated 2004-04-27 19:15
Enter ? for additional hints on searching ARIN's WHOIS databas
e.
—— Querying Reassigned Block: ALASKA WIRELESS CABLE ALAS
KA-W74-102 ——
OrgName: ALASKA WIRELESS CABLE
OrgID: AWC-20
Address: 3055 BRADDOCK STREET
City: FAIRBANKS
StateProv: AK
Show Packet Data Show Rule www.snort.org
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"NETBIOS SMB Data Service Session Setup Anc
IP
Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
12.44.103.112 13.195 4 5 0 457 4500 2 0 115 0
TCP
Source Port Dest Port R1 R0 URG ACK PSH RST SYN FIN Seq # Ack # Offset Res Window Urp ChkSum
2018 445 . . . X X . . . 330510870 151289293 5 0 17122 595 0
DATA
00 00 01 68 FF 53 4D 42 73 00 00 00 00 18 07 C8 ...h.SMBs.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FE ....
01 98 80 00 0C FF 00 68 01 04 41 32 00 00 00 00 ....h..A2....
00 00 00 E4 00 00 00 00 00 D4 00 00 80 2D 01 4E ....-.N
54 4C 4D 53 53 50 00 03 00 00 00 18 00 18 00 A4 TLMSSP..........
00 00 00 18 00 18 00 BC 00 00 00 1E 00 1E 00 40 ....@
00 00 00 28 00 28 00 5E 00 00 00 1E 00 1E 00 86 ...(.(.^........
00 00 00 10 00 10 00 D4 00 00 00 15 82 88 E0 55 ....U
00 53 00 45 00 52 00 2D 00 00 33 .S.E.R.-. .3
00 39 00 38 00 36 00 43 00 45 00 41 00 74 00 52 .9.8.6.C.E.A.t.R
00 32 00 32 00 7A 00 32 00 32 00 62 00 6F 00 61 .2.2.z.2.2.b.o.a
00 74 00 68 00 4C 00 24 00 74 00 68 00 69 00 41 .t.h.L.$.t.h.i.A
00 50 00 26 00 55 00 53 00 45 00 52 00 2D 00 .P.&.U.S.E.R.-.
00 33 00 39 00 38 00 36 00 43 00 45 .3.9.8.6.C.E
00 41 00 1C D4 61 42 86 01 52 E6 00 00 00 00 00 .A...aB..R......
00 00 00 00 00 00 00 00 00 00 00 57 F8 43 DA 19 ...........W.C..
D4 FD 8A 65 18 25 21 93 59 35 74 90 E3 9C 3B F0 ...e.%!.Y5t...;.
41 C8 3F 5B 50 28 5B A2 69 BD 73 90 37 F6 49 DC A.?[P([.i.s.7.I.
56 9A 10 00 57 00 69 00 6E 00 64 00 6F 00 77 00 V...W.i.n.d.o.w.
73 00 20 00 32 00 30 00 30 00 30 00 20 00 32 00 s. .2.0.0.0. .2.
31 00 39 00 35 00 00 00 57 00 69 00 6E 00 64 00 1.9.5...W.i.n.d.
6F 00 77 00 73 00 20 00 32 00 30 00 30 00 30 00 o.w.s. .2.0.0.0.
20 00 35 00 2E 00 30 00 00 00 00 00 00 00 31 .5...0.....1
FF 53 4D 42 2B 00 00 00 00 18 43 C0 00 00 00 00 .SMB+.....C.....
00 00 00 00 00 00 00 00 FF FF FF FE 00 00 FE FF ....
01 01 00 0C 00 4A 6C 4A 6D 49 68 43 6C 42 73 72 .....JlJmIhClBsr
00 .
A user in Alaska is trying to establish SMB connections to port 445 TCP. Is this legitimate?

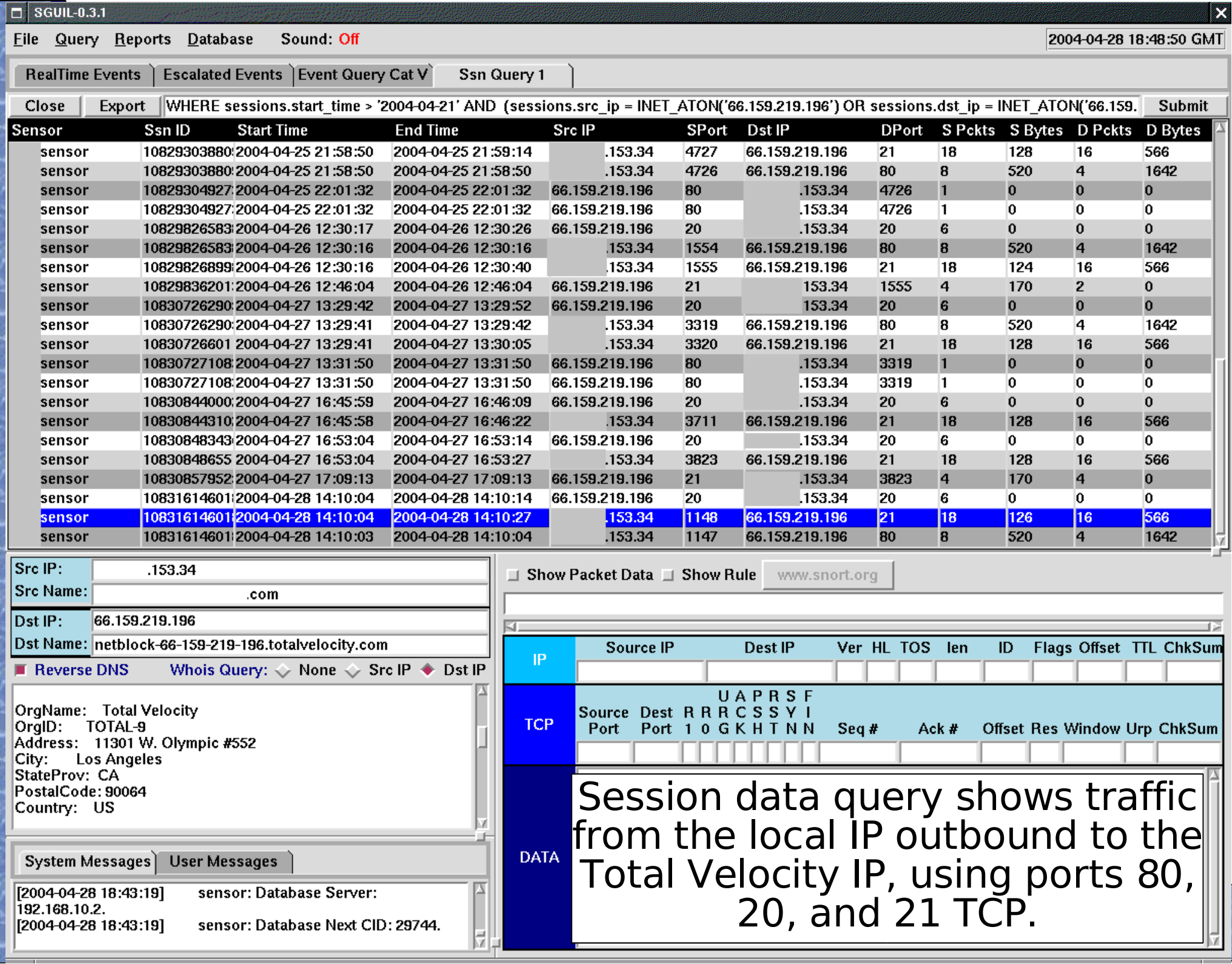

13.195_445-12.44.103.112_2018-6.raw - Ethereal
File Edit View Go Capture Analyze Statistics Help
No. Source Destination Protocol Info
1 12.44.103.112 .13.195 TCP 2018 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
2 .13.195 12.44.103.112 TCP 445 > 2018 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3 12.44.103.112 .13.195 TCP 2018 > 445 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4 12.44.103.112 .13.195 SMB Negotiate Protocol Request
5 .13.195 12.44.103.112 SMB Negotiate Protocol Response
6 .13.195 12.44.103.112 SMB [TCP Retransmission] Negotiate Protocol Response
7 12.44.103.112 .13.195 TCP [TCP Previous segment lost] 2018 > 445 [ACK] Seq=306 Ack=90 Win=17431 Len=0
8 12.44.103.112 .13.195 SMB [TCP Retransmission] Session Setup AndX Request, NTLMSSP_NEGOTIATE
9 .13.195 12.44.103.112 SMB Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10 .13.195 12.44.103.112 SMB [TCP Retransmission] Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE
11 12.44.103.112 .13.195 TCP [TCP Previous segment lost] 2018 > 445 [ACK] Seq=670 Ack=399 Win=17122 Len=0
12 12.44.103.112 .13.195 SMB Echo Request
13 .13.195 12.44.103.112 TCP 445 > 2018 [ACK] Seq=399 Ack=306 Win=65230 Len=0 SLE=544608682 SRE=544608735
14 12.44.103.112 .13.195 SMB [TCP Retransmission] Echo Request
15 .13.195 12.44.103.112 SMB Echo Response
16 .13.195 12.44.103.112 SMB Session Setup AndX Response, Error: STATUS_ACCOUNT_LOCKED_OUT
17 12.44.103.112 .13.195 TCP 2018 > 445 [ACK] Seq=723 Ack=491 Win=17030 Len=0
Ethernet II, Src: 00:06:b1:80:01:10, Dst: 00:0e:84:61:0e:e0
Internet Protocol, Src Addr: .13.195 (.13.195), Dst Addr: 12.44.103.112 (12.44.103.112)
Transmission Control Protocol, Src Port: 445 (445), Dst Port: 2018 (2018), Seq: 452, Ack: 723, Len: 39
NetBIOS Session Service
SMB (Server Message Block Protocol)
SMB Header
Server Component: SMB
Response to: 14
Time from request: 0.002257000 seconds
SMB Command: Session Setup AndX (0x73)
NT Status: STATUS_ACCOUNT_LOCKED_OUT (0xc0000234)
0010 00 4f 6a 52 40 00 80 06 02 cc 0d c3 0c 2c .OjR@... ... ..,
0020 67 70 01 bd 07 e2 5a 2c ea 3c c4 ff f6 82 50 18 gp....Z, .<....P.
0030 fd 2d 0f 7c 00 00 00 00 00 23 ff 53 4d 42 73 34 .-.|.... .#.SMBs4
0040 02 00 c0 98 07 c8 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 ff fe 01 98 80 00 00 00 00 ....
Ethereal follows the entire session and shows this is part of a brute forcing attempt. The target account is locked out.
Filter: Expression... Clear Apply NT Status code (smb.nt_status), P: 53 D: 53 M: 0


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:30:27 GMT
RealTime Events Escalated Events Event Query Cat III Ssn Query 4
Close Export
WHERE sessions.start_time > '2004-04-01' AND (sessions.src_ip = INET_ATON('12.44.103.112') OR sessions.dst_ip = INET_ATON('12.44.103.11
Submit
Sensor Ssn ID Start Time End Time Src IP SPort Dst IP DPort S Pckts S Bytes D Pckts D Bytes
-sensor-va 10814388315 2004-04-08 15:40:31 2004-04-08 15:40:31 12.44.103.112 2065 .13.195 445 7 0 4 0
-sensor-va 10814388813 2004-04-08 15:40:55 2004-04-08 15:41:21 12.44.103.112 2609 .13.195 445 159 21406 126 15658
-sensor-va 10814388850 2004-04-08 15:40:31 2004-04-08 15:40:31 12.44.103.112 2065 .13.195 445 1 0 0 0
-sensor-va 10814388850 2004-04-08 15:40:31 2004-04-08 15:40:34 12.44.103.112 2073 .13.195 445 38 4152 36 5062
-sensor-va 10814389160 2004-04-08 15:40:34 2004-04-08 15:40:56 12.44.103.112 2091 .13.195 445 114 14444 86 10240
-sensor-va 10814389160 2004-04-08 15:41:21 2004-04-08 15:41:21 12.44.103.112 2609 .13.195 445 1 0 0 0
-sensor-va 10814390090 2004-04-08 15:41:21 2004-04-08 15:42:58 12.44.103.112 3182 .13.195 445 1118 153546 866 110938
-sensor-va 10814390400 2004-04-08 15:42:58 2004-04-08 15:43:27 12.44.103.112 1415 .13.195 445 86 11174 66 7996
-sensor-va 10814391330 2004-04-08 15:44:02 2004-04-08 15:44:35 12.44.103.112 2744 .13.195 445 154 20316 122 15502
-sensor-va 10814391330 2004-04-08 15:44:43 2004-04-08 15:44:43 12.44.103.112 3663 .13.200 445 2 0 0 0
-sensor-va 10814391950 2004-04-08 15:45:45 2004-04-08 15:45:48 12.44.103.112 1224 .13.198 445 4 0 0 0
-sensor-va 10814393443 2004-04-08 15:44:41 2004-04-08 15:49:04 12.44.103.112 3714 .13.195 445 2555 348654 1970 253510
-sensor-va 10814393810 2004-04-08 15:49:04 2004-04-08 15:49:04 12.44.103.112 3714 .13.195 445 1 0 0 0
-sensor-va 10814394431 2004-04-08 15:49:23 2004-04-08 15:49:44 12.44.103.112 1967 .13.195 445 218 28718 168 21772
-sensor-va 10814394502 2004-04-08 15:49:45 2004-04-08 15:50:50 12.44.103.112 3161 .13.195 445 53 7174 46 5518
-sensor-va 10814395050 2004-04-08 15:50:50 2004-04-08 15:50:50 12.44.103.112 3161 .13.195 445 1 0 0 0
-sensor-va 10814395360 2004-04-08 15:50:50 2004-04-08 15:51:15 12.44.103.112 2504 .13.195 445 86 10456 68 7840
-sensor-va 10814395980 2004-04-08 15:51:14 2004-04-08 15:52:40 12.44.103.112 3648 .13.195 445 24 1810 18 2188
-sensor-va 10814396910 2004-04-08 15:53:34 2004-04-08 15:53:55 12.44.103.112 2567 .13.195 445 60 6838 42 4822
Src IP: 12.44.103.112
Src Name: wireless103-112.awcable.com
Dst IP: .13.195
Dst Name: .13.195
Reverse DNS Whois Query: None Src IP Dst IP
AT&T WorldNet Services ATT (NET-12-0-0-0-1)
12.0.0.0 - 12.255.255.255
ALASKA WIRELESS CABLE ALASKA-W74-102 (NET-12-44-102-0-1)
12.44.102.0 - 12.44.103.255
ARIN WHOIS database, last updated 2004-04-27 19:15
Enter ? for additional hints on searching ARIN's WHOIS databas
e.
System Messages User Messages
[2004-04-28 18:17:26] sguild: User sguil is monitoring sensors:
-sensor-fl -sensor-va
[2004-04-28 18:24:09] -sensor-fl: /snort_data 10%
Show Packet Data Show Rule www.snort.org
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
TCP Source Port Dest Port R 1 R 0 U R G A C K P S H R S T S Y N F I N Seq # Ack # Offset Res Window Urp ChkSum
DATA
Query for session data shows hundreds of similar sessions to multiple systems.



Adding a Snort rule to knock down connections with TCP RSTs foils a similar brute forcing attack.


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:44:36 GMT
Case 7
RealTime Events Escalated Events Event Qu
Close Export WHERE event.timestamp > '2004-04-01' AND event.status = 15 LIMIT 500 Submit
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
C5 1 sensor 1.28845 2004-04-23 15:40:09 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.28846 2004-04-23 15:40:12 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.28847 2004-04-23 15:40:19 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.28859 2004-04-23 18:57:50 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.28860 2004-04-23 18:57:53 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.28861 2004-04-23 18:58:00 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.28940 2004-04-24 12:15:08 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
Repeated traffic from port 20 to port 20, with no application data. What is this?
C5 1 sensor 1.29004 2004-04-24 21:19:41 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29005 2004-04-24 21:19:44 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29006 2004-04-24 21:19:50 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29095 2004-04-25 21:58:51 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29096 2004-04-25 21:58:54 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29097 2004-04-25 21:59:01 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29160 2004-04-26 12:30:17 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29161 2004-04-26 12:30:20 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
C5 1 sensor 1.29162 2004-04-26 12:30:26 66.159.219.196 20 .153.34 20 6 MISC Source Port 20 to <1024
Src IP: 66.159.219.196
Src Name: netblock-66-159-219-196.totalvelocity.com
Dst IP: .153.34
Dst Name: .com
Reverse DNS Whois Query: None Src IP Dst IP
OrgName: Total Velocity
OrgID: TOTAL-9
Address: 11301 W. Olympic #552
City: Los Angeles
StateProv: CA
PostalCode: 90064
Country: US
Show Packet Data Show Rule www.snort.org
alert tcp $EXTERNAL_NET 20 -> $HOME_NET :1023 (msg:"MISC Source Port 20 to <1024"; flags:S,12;
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
66.159.219.196 .153.34 4 5 0 48 21392 2 0 118 0
TCP Source Port Dest Port R R R U A P R S F 1 0 G K H T N N Seq # Ack # Offset Res Window Urp ChkSum
20 20 . . . . . . X . 300471933 0 7 0 65535 590 0
DATA None.
System Messages User Messages
[2004-04-28 18:43:19] sensor: Database Server: 192.168.10.2.
[2004-04-28 18:43:19] sensor: Database Next CID: 29744.


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-04-28 18:48:50 GMT
RealTime Events Escalated Events Event Query Cat V Ssn Query 1
Close Export WHERE sessions.start_time > '2004-04-21' AND (sessions.src_ip = INET_ATON('66.159.219.196') OR sessions.dst_ip = INET_ATON('66.159. Submit
Sensor Ssn ID Start Time End Time Src IP SPort Dst IP DPort S Pckts S Bytes D Pckts D Bytes
sensor 10829303880 2004-04-25 21:58:50 2004-04-25 21:59:14 .153.34 4727 66.159.219.196 21 18 128 16 566
sensor 10829303880 2004-04-25 21:58:50 2004-04-25 21:58:50 .153.34 4726 66.159.219.196 80 8 520 4 1642
sensor 10829304927 2004-04-25 22:01:32 2004-04-25 22:01:32 66.159.219.196 80 .153.34 4726 1 0 0 0
sensor 10829304927 2004-04-25 22:01:32 2004-04-25 22:01:32 66.159.219.196 80 .153.34 4726 1 0 0 0
sensor 10829826583 2004-04-26 12:30:17 2004-04-26 12:30:26 66.159.219.196 20 .153.34 20 6 0 0 0
sensor 10829826583 2004-04-26 12:30:16 2004-04-26 12:30:16 .153.34 1554 66.159.219.196 80 8 520 4 1642
sensor 10829826899 2004-04-26 12:30:16 2004-04-26 12:30:40 .153.34 1555 66.159.219.196 21 18 124 16 566
sensor 10829836201 2004-04-26 12:46:04 2004-04-26 12:46:04 66.159.219.196 21 153.34 1555 4 170 2 0
sensor 10830726290 2004-04-27 13:29:42 2004-04-27 13:29:52 66.159.219.196 20 153.34 20 6 0 0 0
sensor 10830726290 2004-04-27 13:29:41 2004-04-27 13:29:42 .153.34 3319 66.159.219.196 80 8 520 4 1642
sensor 10830726601 2004-04-27 13:29:41 2004-04-27 13:30:05 .153.34 3320 66.159.219.196 21 18 128 16 566
sensor 10830727108 2004-04-27 13:31:50 2004-04-27 13:31:50 66.159.219.196 80 .153.34 3319 1 0 0 0
sensor 10830727108 2004-04-27 13:31:50 2004-04-27 13:31:50 66.159.219.196 80 .153.34 3319 1 0 0 0
sensor 10830844000 2004-04-27 16:45:59 2004-04-27 16:46:09 66.159.219.196 20 .153.34 20 6 0 0 0
sensor 10830844310 2004-04-27 16:45:58 2004-04-27 16:46:22 .153.34 3711 66.159.219.196 21 18 128 16 566
sensor 10830848343 2004-04-27 16:53:04 2004-04-27 16:53:14 66.159.219.196 20 .153.34 20 6 0 0 0
sensor 10830848655 2004-04-27 16:53:04 2004-04-27 16:53:27 .153.34 3823 66.159.219.196 21 18 128 16 566
sensor 10830857952 2004-04-27 17:09:13 2004-04-27 17:09:13 66.159.219.196 21 .153.34 3823 4 170 4 0
sensor 10831614601 2004-04-28 14:10:04 2004-04-28 14:10:14 66.159.219.196 20 .153.34 20 6 0 0 0
sensor 10831614601 2004-04-28 14:10:04 2004-04-28 14:10:27 .153.34 1148 66.159.219.196 21 18 126 16 566
sensor 10831614601 2004-04-28 14:10:03 2004-04-28 14:10:04 .153.34 1147 66.159.219.196 80 8 520 4 1642
Src IP: .153.34
Src Name: .com
Dst IP: 66.159.219.196
Dst Name: netblock-66-159-219-196.totalvelocity.com
Reverse DNS Whois Query: None Src IP Dst IP
OrgName: Total Velocity
OrgID: TOTAL-9
Address: 11301 W. Olympic #552
City: Los Angeles
StateProv: CA
PostalCode: 90064
Country: US
Show Packet Data Show Rule www.snort.org
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
TCP Source Port Dest Port R R R U A P R S F 1 0 G K H T N N Seq # Ack # Offset Res Window Urp ChkSum
DATA
System Messages User Messages
[2004-04-28 18:43:19] sensor: Database Server: 192.168.10.2.
[2004-04-28 18:43:19] sensor: Database Next CID: 29744.
Session data query shows traffic from the local IP outbound to the Total Velocity IP, using ports 80, 20, and 21 TCP.

sensor_1083161460187786

File

```
Sensor Name:        sensor
Timestamp:          2004-04-28 14:10:04
Connection ID:      sensor_1083161460187786
Src IP:                .153.34     (                          com)
Dst IP:             66.159.219.196     (netblock-66-159-219-196.totalvelocity.com)
Src Port:           1148
Dst Port:           21
================================================================================
======
DST: 220 web2k006 Microsoft FTP Service (Version 5.0).
DST:
SRC: user anonymous
SRC:
DST: 331 Anonymous access allowed, send identity (e-mail name) as password.
DST:
SRC: pass
SRC:
DST: 230 Anonymous user logged in.
DST:
SRC: PORT 10,200,111,36,4,125
SRC:
DST: 500 Invalid PORT Command.
DST:
SRC: RETR
SRC: AddybK.dll
SRC:
DST: 150 Opening ASCII mode data connection for AddybK.dll(62868 bytes).
DST:
DST: 425 Can't open data connection.
DST:
```

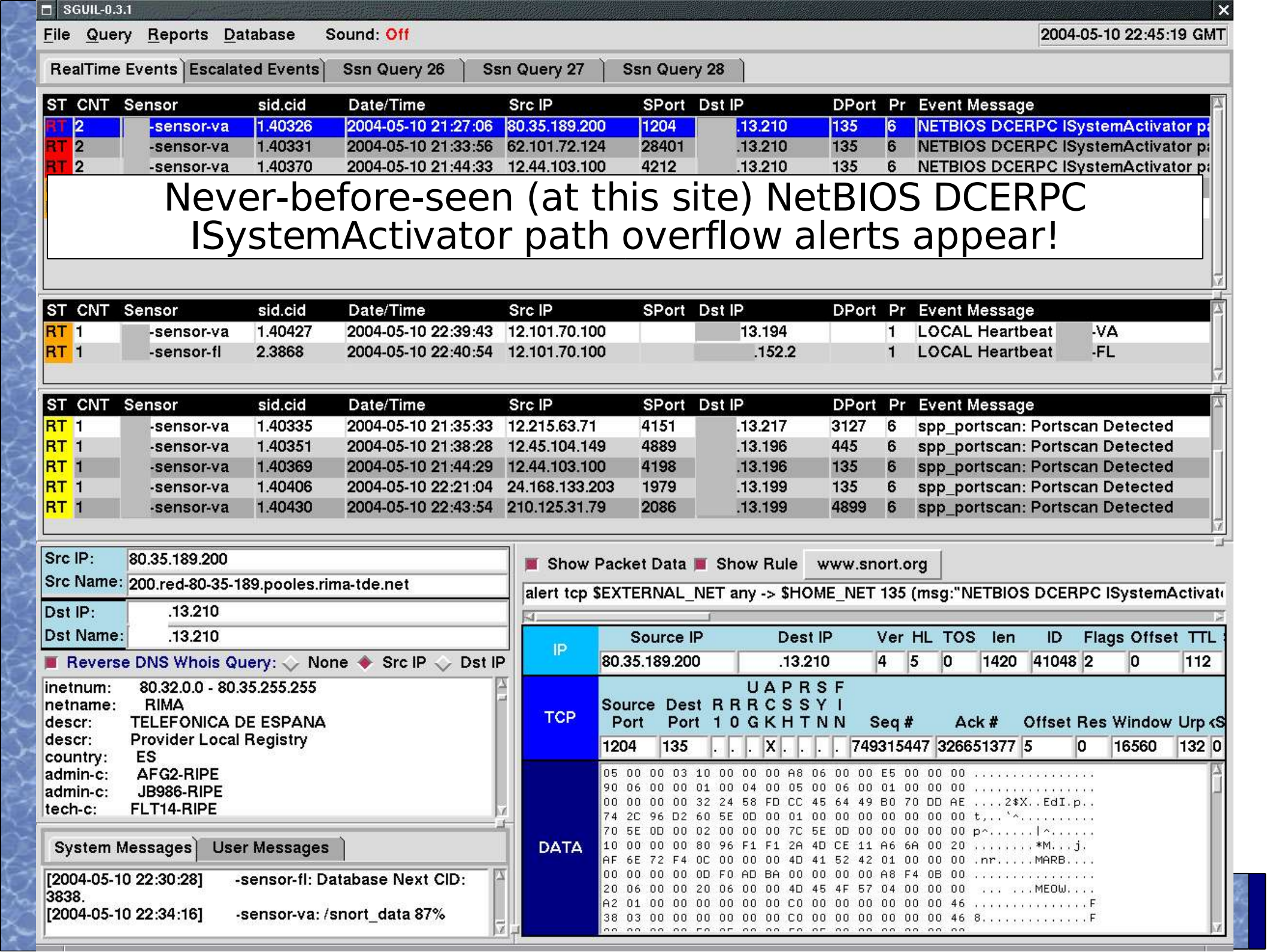
Transcript shows local IP failing to retrieve AddybK.dll; probably infected with malware. Research ties DLL to centralmedia.ws, an adware developer. Note the private source IP in the "PORT" command.

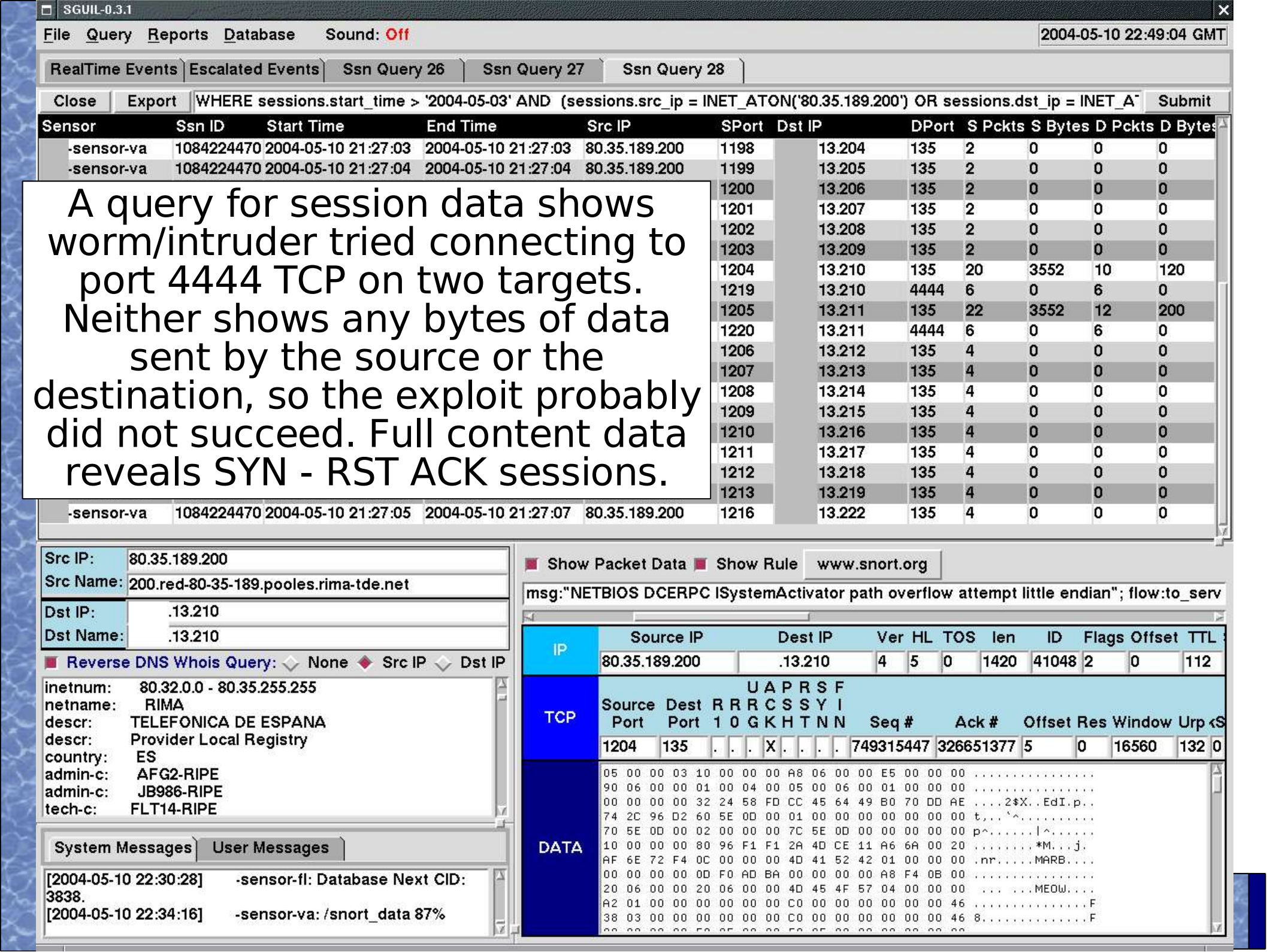
Debug Messages

```
snort.log.1083175200
Creating unique data file on      sensor.
Copying the file from      sensor.
Removing file from      sensor.
```

Bonus Coverage!

As I was preparing this presentation, something changed at a client's site...


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-05-10 22:45:19 GMT
RealTime Events Escalated Events Ssn Query 26 Ssn Query 27 Ssn Query 28
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 2 -sensor-va 1.40326 2004-05-10 21:27:06 80.35.189.200 1204 .13.210 135 6 NETBIOS DCERPC ISystemActivator p
RT 2 -sensor-va 1.40331 2004-05-10 21:33:56 62.101.72.124 28401 .13.210 135 6 NETBIOS DCERPC ISystemActivator p
RT 2 -sensor-va 1.40370 2004-05-10 21:44:33 12.44.103.100 4212 .13.210 135 6 NETBIOS DCERPC ISystemActivator p
Never-before-seen (at this site) NetBIOS DCERPC ISystemActivator path overflow alerts appear!
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 -sensor-va 1.40427 2004-05-10 22:39:43 12.101.70.100 13.194 1 LOCAL Heartbeat -VA
RT 1 -sensor-fl 2.3868 2004-05-10 22:40:54 12.101.70.100 .152.2 1 LOCAL Heartbeat -FL
ST CNT Sensor sid.cid Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 -sensor-va 1.40335 2004-05-10 21:35:33 12.215.63.71 4151 .13.217 3127 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.40351 2004-05-10 21:38:28 12.45.104.149 4889 .13.196 445 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.40369 2004-05-10 21:44:29 12.44.103.100 4198 .13.196 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.40406 2004-05-10 22:21:04 24.168.133.203 1979 .13.199 135 6 spp_portscan: Portscan Detected
RT 1 -sensor-va 1.40430 2004-05-10 22:43:54 210.125.31.79 2086 .13.199 4899 6 spp_portscan: Portscan Detected
Src IP: 80.35.189.200
Src Name: 200.red-80-35-189.pooles.rima-tde.net
Dst IP: .13.210
Dst Name: .13.210
Reverse DNS Whois Query: None Src IP Dst IP
inetnum: 80.32.0.0 - 80.35.255.255
netname: RIMA
descr: TELEFONICA DE ESPANA
descr: Provider Local Registry
country: ES
admin-c: AFG2-RIPE
admin-c: JB986-RIPE
tech-c: FLT14-RIPE
System Messages User Messages
[2004-05-10 22:30:28] -sensor-fl: Database Next CID: 3838.
[2004-05-10 22:34:16] -sensor-va: /snort_data 87%
Show Packet Data Show Rule www.snort.org
alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC ISystemActivat
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL
80.35.189.200 .13.210 4 5 0 1420 41048 2 0 112
TCP Source Port Dest Port R R U A P R S F Seq # Ack # Offset Res Window Urp
1204 135 . . . X 749315447 326651377 5 0 16560 132 0
DATA
05 00 00 03 10 00 00 00 A8 06 00 00 E5 00 00 00 ....
90 06 00 00 01 00 04 00 05 00 06 00 01 00 00 00 ....
00 00 00 00 32 24 58 FD CC 45 64 49 B0 70 DD AE ....2$X..EdI.p..
74 2C 96 D2 60 5E 0D 00 01 00 00 00 00 00 00 00 t,..`^..........
70 5E 0D 00 02 00 00 00 7C 5E 0D 00 00 00 00 00 p^......|^......
10 00 00 00 80 96 F1 F1 2A 4D CE 11 A6 6A 00 20 ....*M...j.
AF 6E 72 F4 0C 00 00 00 4D 41 52 42 01 00 00 00 .nr.....MARB....
00 00 00 00 0D F0 AD BA 00 00 00 00 A8 F4 0B 00 ....
20 06 00 00 20 06 00 00 4D 45 4F 57 04 00 00 00 ... ...MEOW....
A2 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46 ....F
38 03 00 00 00 00 00 00 C0 00 00 00 00 00 00 46 8..............F


SGUIL-0.3.1
File Query Reports Database Sound: Off
2004-05-10 22:49:04 GMT
RealTime Events Escalated Events Ssn Query 26 Ssn Query 27 Ssn Query 28
Close Export WHERE sessions.start_time > '2004-05-03' AND (sessions.src_ip = INET_ATON('80.35.189.200') OR sessions.dst_ip = INET_A Submit
Sensor Ssn ID Start Time End Time Src IP SPort Dst IP DPort S Pckts S Bytes D Pckts D Bytes
-sensor-va 1084224470 2004-05-10 21:27:03 2004-05-10 21:27:03 80.35.189.200 1198 13.204 135 2 0 0 0
-sensor-va 1084224470 2004-05-10 21:27:04 2004-05-10 21:27:04 80.35.189.200 1199 13.205 135 2 0 0 0
1200 13.206 135 2 0 0 0
1201 13.207 135 2 0 0 0
1202 13.208 135 2 0 0 0
1203 13.209 135 2 0 0 0
1204 13.210 135 20 3552 10 120
1219 13.210 4444 6 0 6 0
1205 13.211 135 22 3552 12 200
1220 13.211 4444 6 0 6 0
1206 13.212 135 4 0 0 0
1207 13.213 135 4 0 0 0
1208 13.214 135 4 0 0 0
1209 13.215 135 4 0 0 0
1210 13.216 135 4 0 0 0
1211 13.217 135 4 0 0 0
1212 13.218 135 4 0 0 0
1213 13.219 135 4 0 0 0
-sensor-va 1084224470 2004-05-10 21:27:05 2004-05-10 21:27:07 80.35.189.200 1216 13.222 135 4 0 0 0
A query for session data shows worm/intruder tried connecting to port 4444 TCP on two targets. Neither shows any bytes of data sent by the source or the destination, so the exploit probably did not succeed. Full content data reveals SYN - RST ACK sessions.
Src IP: 80.35.189.200
Src Name: 200.red-80-35-189.pooles.rima-tde.net
Dst IP: .13.210
Dst Name: .13.210
Reverse DNS Whois Query: None Src IP Dst IP
inetnum: 80.32.0.0 - 80.35.255.255
netname: RIMA
descr: TELEFONICA DE ESPANA
descr: Provider Local Registry
country: ES
admin-c: AFG2-RIPE
admin-c: JB986-RIPE
tech-c: FLT14-RIPE
System Messages User Messages
[2004-05-10 22:30:28] -sensor-fl: Database Next CID: 3838.
[2004-05-10 22:34:16] -sensor-va: /snort_data 87%
Show Packet Data Show Rule www.snort.org
msg:"NETBIOS DCERPC ISystemActivator path overflow attempt little endian"; flow:to_serv
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL
80.35.189.200 .13.210 4 5 0 1420 41048 2 0 112
TCP Source Port Dest Port R R R U A P R S F Seq # Ack # Offset Res Window Urp
1204 135 . . . X 749315447 326651377 5 0 16560 132 0
DATA
05 00 00 03 10 00 00 00 A8 06 00 00 E5 00 00 00 ....
90 06 00 00 01 00 04 00 05 00 06 00 01 00 00 00 ....
00 00 00 00 32 24 58 FD CC 45 64 49 B0 70 DD AE ....2$X..EdI.p..
74 2C 96 D2 60 5E 0D 00 01 00 00 00 00 00 00 00 t,..`^..........
70 5E 0D 00 02 00 00 00 7C 5E 0D 00 00 00 00 00 p^......|^......
10 00 00 00 80 96 F1 F1 2A 4D CE 11 A6 6A 00 20 ....*M...j.
AF 6E 72 F4 0C 00 00 00 4D 41 52 42 01 00 00 00 .nr.....MARB....
00 00 00 00 0D F0 AD BA 00 00 00 00 A8 F4 0B 00 ....
20 06 00 00 20 06 00 00 4D 45 4F 57 04 00 00 00 ... ...MEOW....
A2 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46 ....F
38 03 00 00 00 00 00 00 C0 00 00 00 00 00 00 46 8..............F

A more complicated session data query tries to discover why these alerts appeared out of nowhere.

By querying for one of the target IPs, with session bytes > 0, and ignoring ports 80 and 443, we see exactly when the outside world began interacting with newly available ports on this target.

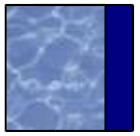
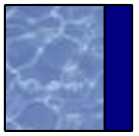
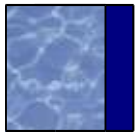
t ns.dst_ip = INET_ATON(' .13.211')) and sessions.dst_bytes > 0 and sessions.dst_port != 80 and sessions.dst_port != 443 Submit

Ssn ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	S Pckts	S Bytes	D Pckts	D Bytes
1084216973	2004-05-10 19:22:52	2004-05-10 19:22:53	216.38.214.96	62061	.13.210	25	24	262	19	868
1084218362	2004-05-10 19:45:01	2004-05-10 19:45:01	12.43.223.29	4452	.13.210	445	12	274	4	178
1084224470	2004-05-10 21:27:04	2004-05-10 21:27:07	80.35.189.200	1204	.13.210	135	20	3552	10	120
1084224836	2004-05-10 21:33:54	2004-05-10 21:33:56	62.101.72.124	28401	.13.210	135	15	3552	14	200
1084225479	2004-05-10 21:44:30	2004-05-10 21:44:39	12.44.103.100	4212	.13.210	135	15	3392	14	280
1084225745	2004-05-10 21:46:06	2004-05-10 21:48:20	81.91.226.43	21048	.13.210	139	14	516	14	8
1084226904	2004-05-10 22:07:24	2004-05-10 22:07:24	12.37.252.76	2231	.13.210	445	12	274	4	178

Thanks again to session data, we can inform the client when a change was made to the access control at the client site.

Future Developments

- Snort rule and sensor management features
- Sguil 0.4.0 offers SANCP (www.metre.net) to replace Snort keepstats session logging
- Augment database output to include PostgreSQL and Oracle
- Test ability to scale
- Rewrite some components in compiled languages
- Live CD or install CDs to ease installation
- FreeBSD port

Questions?

- Thank you for your time.