
PINOY GREYHAT
<< back | track 4
PINOY HACKERS!
THEY DO EXIST

Hashes in Hi-Res
Unleashing the GPU beasts via CUDA

WHOAMI

3ig0nyohB – Pinoy GreyHat Huk

- Total n00b with guts to talk to l33ts
- Can get drunk with pure milk on the table
- Puked on the garden last BT2
- Survivor – survived BlackDawg's vicious bites

Other credentials

- **MIS Manager**
- **Formerly a scene whore**
- **Got 3 kids**
- **Still happily married**
- **Doing talks for Software Freedom Day (http://softwarefreedomday.org)**

Other other credentials

- **Church's Tech Support team**
- **Faith and passion for technology motivated**
- **Wanting to give back to the community**

What's this talk all about

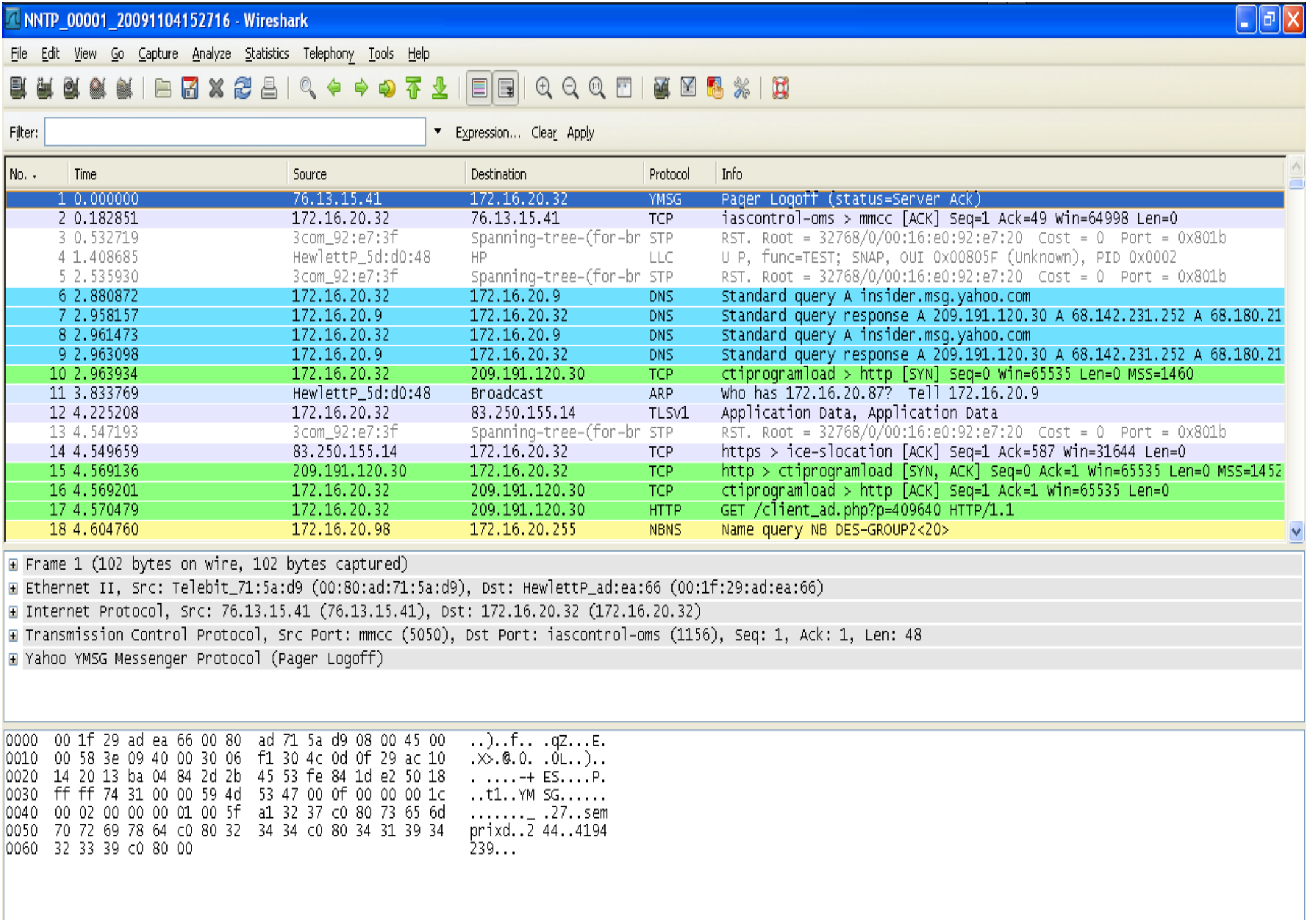
- **NEVER EVER MESS AROUND WITH A HACKER. (they learned the lesson the hard way)**
- **Tackle a little what CUDA is all about**
- **Demo CUDA enabled tools**
- **Q&A Later (No l33t questions please … hehehe)**

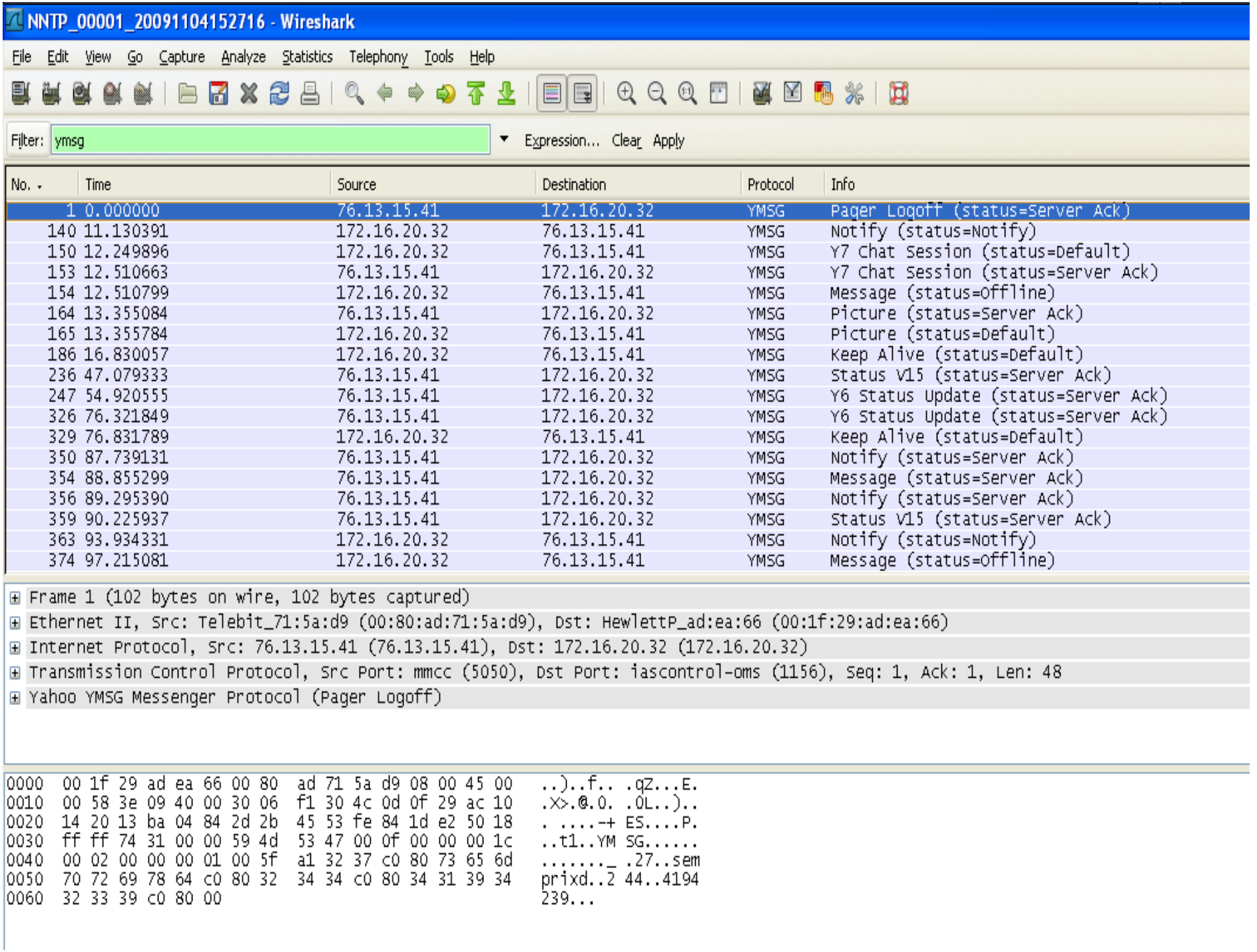
BacktTrack 4
PGHO Release

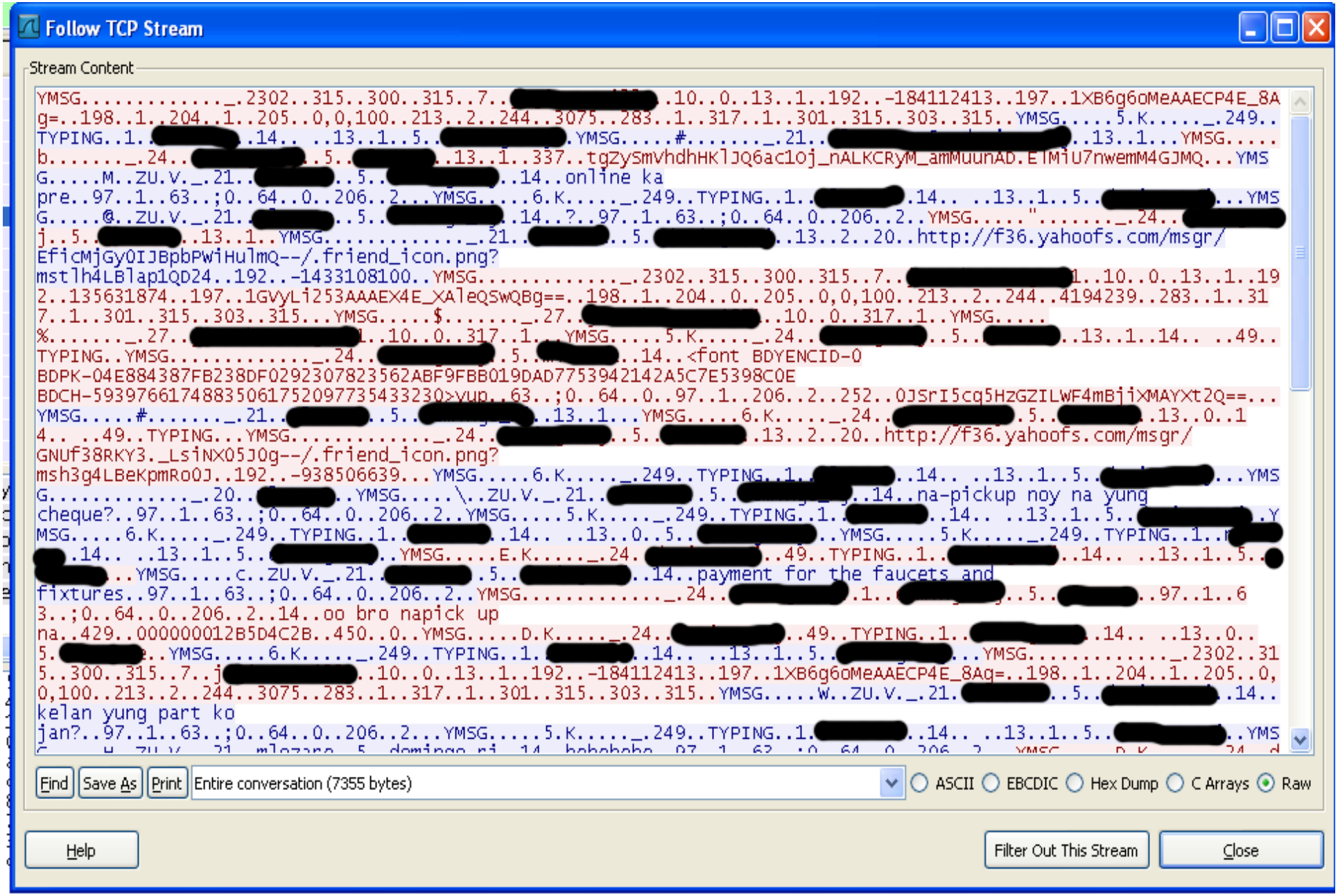
- **Mails are blocked by RBL**
- **Sniffed the whole network – wireshark on the gateway**
- **Analyzed and saved the capture**

- **An a**hole fed the bosses wrong info**
- **I'm moonlighting during/after office hours**
- **Downloading warez**

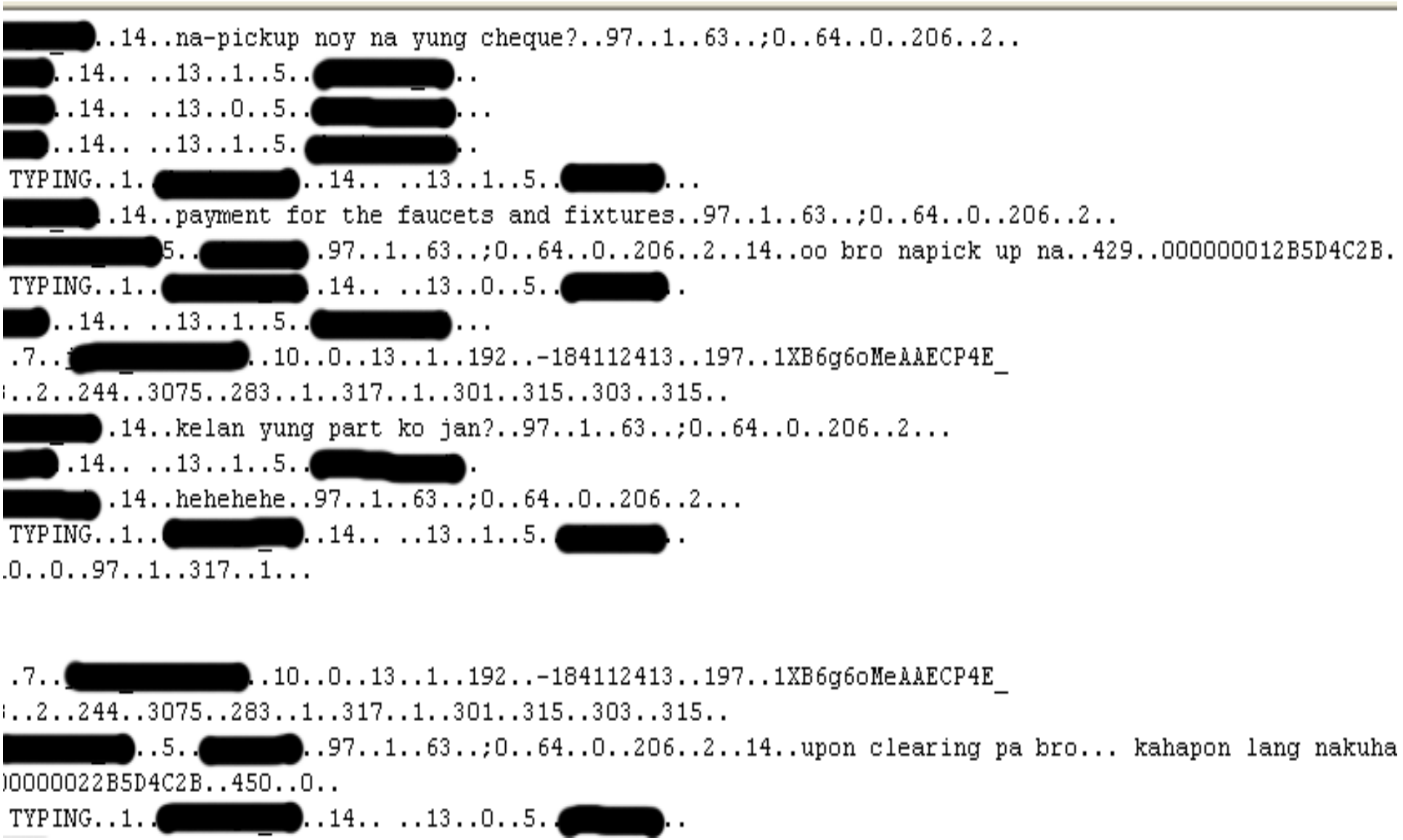
- **Called for closed door meet**
- **Used some SE skillz to win the bosses attention**
- **Showed the captured packets**


NNTP_00001_20091104152716 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 76.13.15.41 172.16.20.32 YMSG Pager Logoff (status=Server Ack)
2 0.182851 172.16.20.32 76.13.15.41 TCP iascontrol-oms > mmcc [ACK] Seq=1 Ack=49 Win=64998 Len=0
3 0.532719 3com_92:e7:3f Spanning-tree-(for-br STP RST. Root = 32768/0/00:16:e0:92:e7:20 Cost = 0 Port = 0x801b
4 1.408685 HewlettP_5d:d0:48 HP LLC U P, func=TEST; SNAP, OUI 0x00805F (Unknown), PID 0x0002
5 2.535930 3com_92:e7:3f Spanning-tree-(for-br STP RST. Root = 32768/0/00:16:e0:92:e7:20 Cost = 0 Port = 0x801b
6 2.880872 172.16.20.32 172.16.20.9 DNS Standard query A insider.msg.yahoo.com
7 2.958157 172.16.20.9 172.16.20.32 DNS Standard query response A 209.191.120.30 A 68.142.231.252 A 68.180.21
8 2.961473 172.16.20.32 172.16.20.9 DNS Standard query A insider.msg.yahoo.com
9 2.963098 172.16.20.9 172.16.20.32 DNS Standard query response A 209.191.120.30 A 68.142.231.252 A 68.180.21
10 2.963934 172.16.20.32 209.191.120.30 TCP ctiprogramload > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
11 3.833769 HewlettP_5d:d0:48 Broadcast ARP Who has 172.16.20.87? Tell 172.16.20.9
12 4.225208 172.16.20.32 83.250.155.14 TLSv1 Application Data, Application Data
13 4.547193 3com_92:e7:3f Spanning-tree-(for-br STP RST. Root = 32768/0/00:16:e0:92:e7:20 Cost = 0 Port = 0x801b
14 4.549659 83.250.155.14 172.16.20.32 TCP https > ice-slocation [ACK] Seq=1 Ack=587 Win=31644 Len=0
15 4.569136 209.191.120.30 172.16.20.32 TCP http > ctiprogramload [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
16 4.569201 172.16.20.32 209.191.120.30 TCP ctiprogramload > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
17 4.570479 172.16.20.32 209.191.120.30 HTTP GET /client_ad.php?p=409640 HTTP/1.1
18 4.604760 172.16.20.98 172.16.20.255 NBNS Name query NB DES-GROUP2<20>
Frame 1 (102 bytes on wire, 102 bytes captured)
Ethernet II, Src: Telebit_71:5a:d9 (00:80:ad:71:5a:d9), Dst: HewlettP_ad:ea:66 (00:1f:29:ad:ea:66)
Internet Protocol, Src: 76.13.15.41 (76.13.15.41), Dst: 172.16.20.32 (172.16.20.32)
Transmission Control Protocol, Src Port: mmcc (5050), Dst Port: iascontrol-oms (1156), Seq: 1, Ack: 1, Len: 48
Yahoo YMSG Messenger Protocol (Pager Logoff)
0000 00 1f 29 ad ea 66 00 80 ad 71 5a d9 08 00 45 00 ..)..f.. .qZ...E.
0010 00 58 3e 09 40 00 30 06 f1 30 4c 0d 0f 29 ac 10 .X>.@.0. .0L..)..
0020 14 20 13 ba 04 84 2d 2b 45 53 fe 84 1d e2 50 18 . ....-+ ES....P.
0030 ff ff 74 31 00 00 59 4d 53 47 00 0f 00 00 00 1c ..t1..YM SG......
0040 00 02 00 00 00 01 00 5f a1 32 37 c0 80 73 65 6d ...._ .27..sem
0050 70 72 69 78 64 c0 80 32 34 34 c0 80 34 31 39 34 prixd..2 44..4194
0060 32 33 39 c0 80 00 239...


NNTP_00001_20091104152716 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: ymsg
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 76.13.15.41 172.16.20.32 YMSG Pager Logoff (status=Server Ack)
140 11.130391 172.16.20.32 76.13.15.41 YMSG Notify (status=Notify)
150 12.249896 172.16.20.32 76.13.15.41 YMSG Y7 Chat Session (status=Default)
153 12.510663 76.13.15.41 172.16.20.32 YMSG Y7 Chat Session (status=Server Ack)
154 12.510799 172.16.20.32 76.13.15.41 YMSG Message (status=Offline)
164 13.355084 76.13.15.41 172.16.20.32 YMSG Picture (status=Server Ack)
165 13.355784 172.16.20.32 76.13.15.41 YMSG Picture (status=Default)
186 16.830057 172.16.20.32 76.13.15.41 YMSG Keep Alive (status=Default)
236 47.079333 76.13.15.41 172.16.20.32 YMSG Status V15 (status=Server Ack)
247 54.920555 76.13.15.41 172.16.20.32 YMSG Y6 Status Update (status=Server Ack)
326 76.321849 76.13.15.41 172.16.20.32 YMSG Y6 Status Update (status=Server Ack)
329 76.831789 172.16.20.32 76.13.15.41 YMSG Keep Alive (status=Default)
350 87.739131 76.13.15.41 172.16.20.32 YMSG Notify (status=Server Ack)
354 88.855299 76.13.15.41 172.16.20.32 YMSG Message (status=Server Ack)
356 89.295390 76.13.15.41 172.16.20.32 YMSG Notify (status=Server Ack)
359 90.225937 76.13.15.41 172.16.20.32 YMSG Status V15 (status=Server Ack)
363 93.934331 172.16.20.32 76.13.15.41 YMSG Notify (status=Notify)
374 97.215081 172.16.20.32 76.13.15.41 YMSG Message (status=Offline)
Frame 1 (102 bytes on wire, 102 bytes captured)
Ethernet II, Src: Telebit_71:5a:d9 (00:80:ad:71:5a:d9), Dst: HewlettP_ad:ea:66 (00:1f:29:ad:ea:66)
Internet Protocol, Src: 76.13.15.41 (76.13.15.41), Dst: 172.16.20.32 (172.16.20.32)
Transmission Control Protocol, Src Port: mmcc (5050), Dst Port: iascontrol-oms (1156), Seq: 1, Ack: 1, Len: 48
Yahoo YMSG Messenger Protocol (Pager Logoff)
0000 00 1f 29 ad ea 66 00 80 ad 71 5a d9 08 00 45 00 ..)..f.. .qZ...E.
0010 00 58 3e 09 40 00 30 06 f1 30 4c 0d 0f 29 ac 10 .X>.@.0. .0L..)..
0020 14 20 13 ba 04 84 2d 2b 45 53 fe 84 1d e2 50 18 . ....-+ ES....P.
0030 ff ff 74 31 00 00 59 4d 53 47 00 0f 00 00 00 1c ..t1..YM SG......
0040 00 02 00 00 00 01 00 5f a1 32 37 c0 80 73 65 6d ...._ .27..sem
0050 70 72 69 78 64 c0 80 32 34 34 c0 80 34 31 39 34 prixd..2 44..4194
0060 32 33 39 c0 80 00 239...


Follow TCP Stream
Stream Content
YMSG.....2302..315..300..315..7..[redacted].10..0..13..1..192..-184112413..197..1XB6g6oMeAAECP4E_8Ag=..198..1..204..1..205..0,0,100..213..2..244..3075..283..1..317..1..301..315..303..315..YMSG.....5.K....._.249..TYPING..1.[redacted].14.. ..13..1..5..[redacted].YMSG.....#....._.21..[redacted]..13..1...YMSG.....b....._.24..[redacted].5..[redacted].13..1..337..tgZySmVhdhHKlJQ6ac1Oj_nALKCRyM_amMuunAD.EIMiU7nwemM4GJMQ...YMSG.....M..ZU.V._.21..[redacted]..5..[redacted]..14..online ka
pre..97..1..63..;0..64..0..206..2...YMSG.....6.K....._.249..TYPING..1..[redacted].14.. ..13..1..5..[redacted]...YMSG.....@..ZU.V._.21..[redacted]..5..[redacted].14..?..97..1..63..;0..64..0..206..2..YMSG.....".....[redacted]
j..5..[redacted]..13..1..YMSG.....[redacted]..21..[redacted]..5..[redacted]..13..2..20..http://f36.yahoofs.com/msgr/EficMjGy0IJBpbPwiHulmQ--/.friend_icon.png?
mstlh4LBlap1QD24..192..-1433108100..YMSG.....[redacted]..10..0..13..1..192..135631874..197..1GVyLi253AAAEX4E_XAleQSwQBg==..198..1..204..0..205..0,0,100..213..2..244..4194239..283..1..317..1..301..315..303..315...YMSG.....$....._.27..[redacted]..10..0..317..1..YMSG.....%....._.27..[redacted]..10..0..317..1..YMSG.....5.K....._.24..[redacted]..5..[redacted]..13..1..14.. ..49..TYPING..YMSG.....[redacted]..5..[redacted]..14..<font BDYENCID=0
BDPK=04E884387FB238DF0292307823562ABF9FBB019DAD7753942142A5C7E5398C0E
BDCH=59397661748835061752097735433230>yup..63..;0..64..0..97..1..206..2..252..0JSrI5cq5HzGZILWF4mBjiXMAYXt2Q==...YMSG.....#....._.21..[redacted]..5..[redacted]..13..1...YMSG.....6.K....._.24..[redacted].5..[redacted].13..0..14.. ..49..TYPING...YMSG.....[redacted]..5..[redacted].13..2..20..http://f36.yahoofs.com/msgr/GNUf38RKY3._LsiNX05JOg--/.friend_icon.png?
msh3g4LBeKpmRo0J..192..-938506639...YMSG.....6.K....._.249..TYPING..1..[redacted]..14.. ..13..1..5..[redacted]...YMSG.....[redacted]..20..[redacted]..YMSG.....\..ZU.V._.21..[redacted].5..[redacted]..14..na-pickup noy na yung cheque?..97..1..63..;0..64..0..206..2..YMSG.....5.K....._.249..TYPING..1..[redacted]..14.. ..13..1..5..[redacted].YMSG.....6.K....._.249..TYPING..1..[redacted]..14.. ..13..0..5..[redacted]..YMSG.....5.K....._.249..TYPING..1..[redacted]..14.. ..13..1..5..[redacted]..YMSG.....E.K....._.24..[redacted]..49..TYPING..1..[redacted]..14.. ..13..1..5..[redacted]..YMSG.....c..ZU.V._.21..[redacted].5..[redacted]..14..payment for the faucets and fixtures..97..1..63..;0..64..0..206..2..YMSG.....[redacted].1..[redacted]..5..[redacted]..97..1..63..;0..64..0..206..2..14..oo bro napick up
na..429..000000012B5D4C2B..450..0..YMSG.....D.K....._.24..[redacted]..49..TYPING..1..[redacted].14.. ..13..0..5.[redacted]..YMSG.....6.K....._.249..TYPING..1..[redacted]..14.. ..13..1..5..[redacted]...YMSG.....[redacted]..10..0..13..1..192..-184112413..197..1XB6g6oMeAAECP4E_8Ag=..198..1..204..1..205..0,0,100..213..2..244..3075..283..1..317..1..301..315..303..315..YMSG.....W..ZU.V._.21..[redacted]..5..[redacted].14..kelan yung part ko
jan?..97..1..63..;0..64..0..206..2...YMSG.....5.K....._.249..TYPING..1..[redacted]..14.. ..13..1..5..[redacted]..YMS
Find
Save As
Print
Entire conversation (7355 bytes)
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

Accidentally? showed a .... hehehehe



[redacted]..14..0x3..97..1..63..;0..64..0..206..2..
[redacted]..49..TYPING..1.[redacted]..14.. ..13..1..5..[redacted].
..1.[redacted]..14.. ..13..1..5.[redacted]...
..5..[redacted]..14..balitaan mo pag okay na yung com ko..97..1..63..;0..64..0..206..2...
..1.[redacted].14.. ..13..1..5..[redacted]...
..
..5..[redacted]..14..pickup ko jan..97..1..63..;0..64..0..206..2..
1.1.[redacted].14.. ..13..1..5.[redacted]...
300..315..7..[redacted].10..0..13..1..192..-184112413..197..1XB6g6oMeAAECP4E_
,100..213..2..244..3075..283..1..317..1..301..315..303..315..
..5..[redacted]..14..:D..97..1..63..;0..64..0..206..2...
[redacted]..1..[redacted]..5..[redacted]..97..1..63..;0..64..0..206..2..14..naninigurado lang naman..
50..0...
[redacted]..49..TYPING..1.[redacted]..14.. ..13..0..5..[redacted].
[redacted]..49..TYPING..1..[redacted].14.. ..13..1..5..[redacted]..
[redacted]

THE ASSHOLE GOT HIS ASS KICKED

NEVER EVER MESS AROUND WITH A HACKER. They learned their lessons the hard way.

Hashes in Hi-Res

The old times

- **Use JTR to break hashes**
- **Cain and Abel**
- **Aircrack-NG**
- **Cowpatty**
- **Ophcrack+Online Rainbow Tables**

Problem with old times

- JTR takes a long time breaking complex/non-dict passwords
- "djohnd" exists but nodes should have similar CPU power – expensive to build
- Aircrack-NG is the same (or used to be the same)
- Cowpatty – space hog
- Online Rainbow tables – Waiting list is as long as people in Divisoria during holiday season

Enter CUDA

- **Compute Unified Device Architecture**
- **CUDA – parallel computing architecture by NVIDIA**
- **leverages the parallel compute engine in NVIDIA GPUs**
- **In other words … It's l33t (but a n00b is talking about it now)**

Why CUDA?

- **Can break hashes 10 to 15 times using CUDA enabled apps**
- **Can crack hashes faster when combined with Space-Time-Trade-Off**
- **Tools are already scattered and being developed to take advantage of this technology**
- **It's ready to roll on BT4**

CUDA Enabled tools

- **Multiforcer – MD5, MD4, NTLM/2 brute forcer**
- **BarsWF (MD5 only) – MD5 bruteforcer for windows**
- **Pyrit – latest attack tool on Wireless encryptions**
- **Aircrack-NG now supports CUDA – not enabled by default**

Multiforcer Demo

Pyrit

Pyrit + CUDA

Pyrit + cowpatty

Credits

- Encrypted and aphro.ph of PGHO
- Pureh@te Of remote-exploit – I used his paper for this talk
- People at aircrack-ng.org
- Bitweasil of cryptohaze.com for multiforcer
- lucas.lueg - author of pyrit
- The whole remote-exploit team
- Church of WiFi congregation
- PINOYGREYHAT.ORG community