Taiwan Malware Analysis Net+, TWMAN+ - Analysis Report
臺灣惡意程式分析網+，抬丸郎+ - 分析報告 2012-03-15 版
Cored By Truman 0.1, Developed By TonTon
Offical Web: http:://TWAN.ORG | Mail: TonTon@TWMAN.ORG

>> Report for d93efa9141593bc8cea045d080ed5658 created at 二 3月 20 19:33:54 GMT 2012 <<

>> Memorydump info of Volatility Framework <<
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP3x86, WinXPSP2x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace
(/forensics/d93efa9141593bc8cea045d080ed5658/d93efa9141593bc8cea045d080ed5658.img)
                      PAE type : PAE
                           DTB : 0xbe9000
                          KDBG : 0x80546ae0L
                          KPCR : 0xffdff000L
            KUSER_SHARED_DATA : 0xffdf0000L
          Image date and time : 2012-03-20 18:44:26
     Image local date and time : 2012-03-20 18:44:26
          Number of Processors : 1
                    Image Type : Service Pack 3

>> Host file changes <<

>> Registry Run Key changes <<

>> Registry Service Key changes <<

>> Hivelist of Volatility Framework<<
Virtual   Physical   Name
0xe2517510 0x0d9bf510 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
0xe24ed5b8 0x0daac5b8 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe215d008 0x0d1b7008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
0xe2155518 0x0cfa4518 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe2135078 0x0ce89078 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
0xe212f008 0x0ce7b008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1dc06b8 0x08f696b8 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1dbf228 0x08c55228 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe13e5b60 0x033deb60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe1dc0b60 0x08f69b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe12a4288 0x01d9f288 [no name]
0xe1019498 0x01b11498 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008b60 0x01b05b60 [no name]
0x80671a0c 0x00671a0c [no name]

>> Process Tree of Volatility Framework <<
Name   Pid   PPid   Thds   Hnds   Time
 0x8116EDA0:System   4   0   61   373 1970-01-01 00:00:00
. 0xFF0BB608:smss.exe   472   4   3   19 2012-03-20 18:42:17
.. 0xFF06A758:csrss.exe   640   472   12   389 2012-03-20 18:42:18
.. 0xFF040020:winlogon.exe   664   472   21   443 2012-03-20 18:42:21
... 0xFEF46020:taskmgr.exe   1424   664   3   80 2012-03-20 18:42:51
... 0xFF03EAB8:services.exe   932   664   16   249 2012-03-20 18:42:22
.... 0x8106F558:svchost.exe   1432   932   14   195 2012-03-20 18:42:23
.... 0xFEFEF840:svchost.exe   1180   932   10   241 2012-03-20 18:42:22
.... 0xFEFE5020:svchost.exe   1324   932   76   1221 2012-03-20 18:42:23
..... 0xFEF4A020:wscntfy.exe   572   1324   1   38 2012-03-20 18:42:38
..... 0xFEFB3488:wuauclt.exe   420   1324   8   173 2012-03-20 18:43:22
.... 0xFF0018B0:svchost.exe   1104   932   20   204 2012-03-20 18:42:22
.... 0xFEFA1AA8:spoolsv.exe   340   932   14   111 2012-03-20 18:42:25
.... 0xFEFE1AF8:svchost.exe   1376   932   6   82 2012-03-20 18:42:23
.... 0xFEF43B28:alg.exe   760   932   7   104 2012-03-20 18:42:39
... 0xFF045BB8:lsass.exe   944   664   24   334 2012-03-20 18:42:22
 0xFEFAFC88:explorer.exe   1928   1900   14   383 2012-03-20 18:42:24
. 0x80FCF5F8:cmd.exe   1736   1928   1   35 2012-03-20 18:44:21
.. 0x81051DA0:dd.exe   2012   1736   1   21 2012-03-20 18:44:26
.. 0x81124DA0:conime.exe   1124   1736   1   36 2012-03-20 18:44:21
. 0xFFB532D8:igfxtray.exe   220   1928   4   80 2012-03-20 18:42:38
. 0x81064DA0:hkcmd.exe   228   1928   4   88 2012-03-20 18:42:38
. 0xFFB46C10:igfxpers.exe   236   1928   6   96 2012-03-20 18:42:38
. 0xFFB73DA0:ctfmon.exe   244   1928   1   69 2012-03-20 18:42:38

>> Hunting rootkits and malicious code of Volatility Framework <<
Name   Pid   Start   End   Tag   Hits   Protect

>> ssdeep info (Fuzzy Hashing)<<
6144:wZ+RwPONXoRjDhIcp0fDlavx+W26nAeTk+HaidN4NVzZPYK51kl+imH6LpkTwkpM:eLHaa0zZjDkl+imH69kwkp7sCdxDXoBV,"d93efa9141593bc8
cea045d080ed5658"

```
>> Firewall changes <<

>> Network Connection of Volatility Framework <<

>> Network Connection <<
IP 192.168.0.110.9371 > 65.6.163.4.50144: UDP, length 74
IP 192.168.0.110.9371 > 89.123.188.11.8957: UDP, length 74
IP 192.168.0.110.9371 > 90.52.108.231.58856: UDP, length 74
IP 192.168.0.110.9371 > 85.11.66.73.38338: UDP, length 74
IP 192.168.0.110.9371 > 72.192.20.73.16306: UDP, length 74
IP 192.168.0.110.9371 > 219.77.13.11.22137: UDP, length 74
IP 192.168.0.110.9371 > 90.201.190.208.25439: UDP, length 74
IP 192.168.0.110.9371 > 58.63.39.204.40139: UDP, length 74
IP 192.168.0.110.9371 > 77.66.224.30.30478: UDP, length 74
IP 192.168.0.110.9371 > 62.65.208.112.9342: UDP, length 74
IP 192.168.0.110 > 192.168.1.0: ICMP echo request, id 12293, seq 3277, length 44
IP 192.168.0.110 > 192.168.1.0: ICMP echo request, id 12293, seq 62672, length 44
IP 192.168.0.110 > 192.168.1.1: ICMP echo request, id 12293, seq 56532, length 44
IP 192.168.0.110 > 192.168.1.1: ICMP echo request, id 12293, seq 50392, length 44
IP 192.168.0.110 > 192.168.1.2: ICMP echo request, id 12293, seq 44252, length 44
IP 192.168.0.110 > 192.168.1.2: ICMP echo request, id 12293, seq 38112, length 44
IP 192.168.0.110 > 192.168.1.3: ICMP echo request, id 12293, seq 31972, length 44
IP 192.168.0.110 > 192.168.1.3: ICMP echo request, id 12293, seq 25832, length 44
IP 192.168.0.110 > 192.168.1.4: ICMP echo request, id 12293, seq 19692, length 44
IP 192.168.0.110 > 192.168.1.4: ICMP echo request, id 12293, seq 13552, length 44
IP 192.168.0.110 > 192.168.1.5: ICMP echo request, id 12293, seq 7412, length 44
IP 192.168.0.110 > 192.168.1.5: ICMP echo request, id 12293, seq 1272, length 44
IP 192.168.0.110 > 192.168.1.6: ICMP echo request, id 12293, seq 60667, length 44
IP 192.168.0.110 > 192.168.1.6: ICMP echo request, id 12293, seq 54527, length 44
IP 192.168.0.110 > 192.168.1.7: ICMP echo request, id 12293, seq 48131, length 44
IP 192.168.0.110 > 192.168.1.7: ICMP echo request, id 12293, seq 41991, length 44
IP 192.168.0.110 > 192.168.1.8: ICMP echo request, id 12293, seq 35851, length 44
IP 192.168.0.110 > 192.168.1.8: ICMP echo request, id 12293, seq 29711, length 44
IP 192.168.0.110 > 192.168.1.9: ICMP echo request, id 12293, seq 23571, length 44
IP 192.168.0.110 > 192.168.1.9: ICMP echo request, id 12293, seq 17431, length 44
IP 192.168.0.110 > 192.168.1.10: ICMP echo request, id 12293, seq 11291, length 44
IP 192.168.0.110 > 192.168.1.10: ICMP echo request, id 12293, seq 5151, length 44
IP 192.168.0.110 > 192.168.1.11: ICMP echo request, id 12293, seq 64546, length 44
IP 192.168.0.110 > 192.168.1.11: ICMP echo request, id 12293, seq 58406, length 44
IP 192.168.0.110 > 192.168.1.12: ICMP echo request, id 12293, seq 52266, length 44
IP 192.168.0.110 > 192.168.1.12: ICMP echo request, id 12293, seq 46126, length 44
IP 192.168.0.110 > 192.168.1.13: ICMP echo request, id 12293, seq 39986, length 44
IP 192.168.0.110 > 192.168.1.13: ICMP echo request, id 12293, seq 33846, length 44
IP 192.168.0.110 > 192.168.1.14: ICMP echo request, id 12293, seq 27706, length 44
IP 192.168.0.110 > 192.168.1.14: ICMP echo request, id 12293, seq 21566, length 44
IP 192.168.0.110 > 192.168.1.15: ICMP echo request, id 12293, seq 15426, length 44
IP 192.168.0.110 > 192.168.1.15: ICMP echo request, id 12293, seq 9286, length 44
IP 192.168.0.110 > 192.168.1.16: ICMP echo request, id 12293, seq 3146, length 44
IP 192.168.0.110 > 192.168.1.16: ICMP echo request, id 12293, seq 62541, length 44
IP 192.168.0.110 > 192.168.1.17: ICMP echo request, id 12293, seq 56401, length 44
IP 192.168.0.110 > 192.168.1.17: ICMP echo request, id 12293, seq 50261, length 44
IP 192.168.0.110 > 192.168.1.18: ICMP echo request, id 12293, seq 44121, length 44
IP 192.168.0.110 > 192.168.1.18: ICMP echo request, id 12293, seq 37981, length 44
IP 192.168.0.110 > 192.168.1.19: ICMP echo request, id 12293, seq 31841, length 44
IP 192.168.0.110 > 192.168.1.19: ICMP echo request, id 12293, seq 25701, length 44
IP 192.168.0.110 > 192.168.1.20: ICMP echo request, id 12293, seq 19561, length 44
IP 192.168.0.110 > 192.168.1.20: ICMP echo request, id 12293, seq 13421, length 44
IP 192.168.0.110 > 192.168.1.21: ICMP echo request, id 12293, seq 7281, length 44
IP 192.168.0.110 > 192.168.1.21: ICMP echo request, id 12293, seq 1141, length 44
IP 192.168.0.110 > 192.168.1.22: ICMP echo request, id 12293, seq 60536, length 44
IP 192.168.0.110 > 192.168.1.22: ICMP echo request, id 12293, seq 54396, length 44
IP 192.168.0.110 > 192.168.1.23: ICMP echo request, id 12293, seq 48256, length 44
IP 192.168.0.110 > 192.168.1.23: ICMP echo request, id 12293, seq 42116, length 44
IP 192.168.0.110 > 192.168.1.24: ICMP echo request, id 12293, seq 35976, length 44
IP 192.168.0.110 > 192.168.1.24: ICMP echo request, id 12293, seq 29836, length 44
IP 192.168.0.110 > 192.168.1.25: ICMP echo request, id 12293, seq 23696, length 44
IP 192.168.0.110 > 192.168.1.25: ICMP echo request, id 12293, seq 17556, length 44
IP 192.168.0.110 > 192.168.1.26: ICMP echo request, id 12293, seq 11416, length 44
IP 192.168.0.110 > 192.168.1.26: ICMP echo request, id 12293, seq 5276, length 44
IP 192.168.0.110 > 192.168.1.27: ICMP echo request, id 12293, seq 64671, length 44
IP 192.168.0.110 > 192.168.1.27: ICMP echo request, id 12293, seq 58531, length 44
IP 192.168.0.110 > 192.168.1.28: ICMP echo request, id 12293, seq 52391, length 44
IP 192.168.0.110 > 192.168.1.28: ICMP echo request, id 12293, seq 46251, length 44
IP 192.168.0.110 > 192.168.1.29: ICMP echo request, id 12293, seq 40111, length 44
IP 192.168.0.110 > 192.168.1.29: ICMP echo request, id 12293, seq 33971, length 44
IP 192.168.0.110 > 192.168.1.30: ICMP echo request, id 12293, seq 27831, length 44
IP 192.168.0.110 > 192.168.1.30: ICMP echo request, id 12293, seq 21691, length 44
IP 192.168.0.110 > 192.168.1.31: ICMP echo request, id 12293, seq 15551, length 44
IP 192.168.0.110 > 192.168.1.31: ICMP echo request, id 12293, seq 9411, length 44
IP 192.168.0.110 > 192.168.1.32: ICMP echo request, id 12293, seq 3271, length 44
IP 192.168.0.110 > 192.168.1.32: ICMP echo request, id 12293, seq 62666, length 44
IP 192.168.0.110 > 192.168.1.33: ICMP echo request, id 12293, seq 56526, length 44
IP 192.168.0.110 > 192.168.1.33: ICMP echo request, id 12293, seq 50386, length 44
IP 192.168.0.110 > 192.168.1.34: ICMP echo request, id 12293, seq 44246, length 44
IP 192.168.0.110 > 192.168.1.34: ICMP echo request, id 12293, seq 38106, length 44
IP 192.168.0.110 > 192.168.1.35: ICMP echo request, id 12293, seq 31966, length 44
IP 192.168.0.110 > 192.168.1.35: ICMP echo request, id 12293, seq 25826, length 44
IP 192.168.0.110 > 192.168.1.36: ICMP echo request, id 12293, seq 19686, length 44
```

```
IP 192.168.0.110 > 192.168.1.36: ICMP echo request, id 12293, seq 13546, length 44
IP 192.168.0.110 > 192.168.1.37: ICMP echo request, id 12293, seq 7406, length 44
IP 192.168.0.110 > 192.168.1.37: ICMP echo request, id 12293, seq 1266, length 44
IP 192.168.0.110 > 192.168.1.38: ICMP echo request, id 12293, seq 60661, length 44
IP 192.168.0.110 > 192.168.1.38: ICMP echo request, id 12293, seq 54521, length 44
IP 192.168.0.110 > 192.168.1.39: ICMP echo request, id 12293, seq 48381, length 44
IP 192.168.0.110 > 192.168.1.39: ICMP echo request, id 12293, seq 41985, length 44
IP 192.168.0.110 > 192.168.1.40: ICMP echo request, id 12293, seq 35845, length 44
IP 192.168.0.110 > 192.168.1.40: ICMP echo request, id 12293, seq 29705, length 44
IP 192.168.0.110 > 192.168.1.41: ICMP echo request, id 12293, seq 23565, length 44
IP 192.168.0.110 > 192.168.1.41: ICMP echo request, id 12293, seq 17425, length 44
IP 192.168.0.110 > 192.168.1.42: ICMP echo request, id 12293, seq 11285, length 44
IP 192.168.0.110 > 192.168.1.42: ICMP echo request, id 12293, seq 5145, length 44
IP 192.168.0.110 > 192.168.1.43: ICMP echo request, id 12293, seq 64540, length 44
IP 192.168.0.110 > 192.168.1.43: ICMP echo request, id 12293, seq 58400, length 44
IP 192.168.0.110 > 192.168.1.44: ICMP echo request, id 12293, seq 52260, length 44
IP 192.168.0.110 > 192.168.1.44: ICMP echo request, id 12293, seq 46120, length 44
IP 192.168.0.110 > 192.168.1.45: ICMP echo request, id 12293, seq 39980, length 44
IP 192.168.0.110 > 192.168.1.45: ICMP echo request, id 12293, seq 33840, length 44
IP 192.168.0.110 > 192.168.1.46: ICMP echo request, id 12293, seq 27700, length 44
IP 192.168.0.110 > 192.168.1.46: ICMP echo request, id 12293, seq 21560, length 44
IP 192.168.0.110 > 192.168.1.47: ICMP echo request, id 12293, seq 15420, length 44
IP 192.168.0.110 > 192.168.1.47: ICMP echo request, id 12293, seq 9280, length 44
IP 192.168.0.110 > 192.168.1.48: ICMP echo request, id 12293, seq 3140, length 44
IP 192.168.0.110 > 192.168.1.48: ICMP echo request, id 12293, seq 62535, length 44
IP 192.168.0.110 > 192.168.1.49: ICMP echo request, id 12293, seq 56395, length 44
IP 192.168.0.110 > 192.168.1.49: ICMP echo request, id 12293, seq 50255, length 44
IP 192.168.0.110 > 192.168.1.50: ICMP echo request, id 12293, seq 44115, length 44
IP 192.168.0.110 > 192.168.1.50: ICMP echo request, id 12293, seq 37975, length 44
IP 192.168.0.110 > 192.168.1.51: ICMP echo request, id 12293, seq 31835, length 44
IP 192.168.0.110 > 192.168.1.51: ICMP echo request, id 12293, seq 25695, length 44
IP 192.168.0.110 > 192.168.1.52: ICMP echo request, id 12293, seq 19555, length 44
IP 192.168.0.110 > 192.168.1.52: ICMP echo request, id 12293, seq 13415, length 44
IP 192.168.0.110 > 192.168.1.53: ICMP echo request, id 12293, seq 7275, length 44
IP 192.168.0.110 > 192.168.1.53: ICMP echo request, id 12293, seq 1135, length 44
IP 192.168.0.110 > 192.168.1.54: ICMP echo request, id 12293, seq 60530, length 44
IP 192.168.0.110 > 192.168.1.54: ICMP echo request, id 12293, seq 54390, length 44
IP 192.168.0.110 > 192.168.1.55: ICMP echo request, id 12293, seq 48250, length 44
IP 192.168.0.110 > 192.168.1.55: ICMP echo request, id 12293, seq 42110, length 44
IP 192.168.0.110 > 192.168.1.56: ICMP echo request, id 12293, seq 35970, length 44
IP 192.168.0.110 > 192.168.1.56: ICMP echo request, id 12293, seq 29830, length 44
IP 192.168.0.110 > 192.168.1.57: ICMP echo request, id 12293, seq 23690, length 44
IP 192.168.0.110 > 192.168.1.57: ICMP echo request, id 12293, seq 17550, length 44
IP 192.168.0.110 > 192.168.1.58: ICMP echo request, id 12293, seq 11410, length 44
IP 192.168.0.110 > 192.168.1.58: ICMP echo request, id 12293, seq 5270, length 44
IP 192.168.0.110 > 192.168.1.59: ICMP echo request, id 12293, seq 64665, length 44
IP 192.168.0.110 > 192.168.1.59: ICMP echo request, id 12293, seq 58525, length 44
IP 192.168.0.110 > 192.168.1.60: ICMP echo request, id 12293, seq 52385, length 44
IP 192.168.0.110 > 192.168.1.60: ICMP echo request, id 12293, seq 46245, length 44
IP 192.168.0.110 > 192.168.1.61: ICMP echo request, id 12293, seq 40105, length 44
IP 192.168.0.110 > 192.168.1.61: ICMP echo request, id 12293, seq 33965, length 44
IP 192.168.0.110 > 192.168.1.62: ICMP echo request, id 12293, seq 27825, length 44
IP 192.168.0.110 > 192.168.1.62: ICMP echo request, id 12293, seq 21685, length 44
IP 192.168.0.110 > 192.168.1.63: ICMP echo request, id 12293, seq 15545, length 44
IP 192.168.0.110 > 192.168.1.63: ICMP echo request, id 12293, seq 9405, length 44
IP 192.168.0.110 > 192.168.1.64: ICMP echo request, id 12293, seq 3265, length 44
IP 192.168.0.110 > 192.168.1.64: ICMP echo request, id 12293, seq 62660, length 44
IP 192.168.0.110 > 192.168.1.65: ICMP echo request, id 12293, seq 56520, length 44
IP 192.168.0.110 > 192.168.1.65: ICMP echo request, id 12293, seq 50380, length 44
IP 192.168.0.110 > 192.168.1.66: ICMP echo request, id 12293, seq 44240, length 44
IP 192.168.0.110 > 192.168.1.66: ICMP echo request, id 12293, seq 38100, length 44
IP 192.168.0.110 > 192.168.1.67: ICMP echo request, id 12293, seq 31960, length 44
IP 192.168.0.110 > 192.168.1.67: ICMP echo request, id 12293, seq 25820, length 44
IP 192.168.0.110 > 192.168.1.68: ICMP echo request, id 12293, seq 19680, length 44
IP 192.168.0.110 > 192.168.1.68: ICMP echo request, id 12293, seq 13540, length 44
IP 192.168.0.110 > 192.168.1.69: ICMP echo request, id 12293, seq 7400, length 44
IP 192.168.0.110 > 192.168.1.69: ICMP echo request, id 12293, seq 1260, length 44
IP 192.168.0.110 > 192.168.1.70: ICMP echo request, id 12293, seq 60655, length 44
IP 192.168.0.110 > 192.168.1.70: ICMP echo request, id 12293, seq 54515, length 44
IP 192.168.0.110 > 192.168.1.71: ICMP echo request, id 12293, seq 48375, length 44
IP 192.168.0.110 > 192.168.1.71: ICMP echo request, id 12293, seq 42235, length 44
IP 192.168.0.110 > 192.168.1.72: ICMP echo request, id 12293, seq 36095, length 44
IP 192.168.0.110 > 192.168.1.72: ICMP echo request, id 12293, seq 29699, length 44
IP 192.168.0.110 > 192.168.1.73: ICMP echo request, id 12293, seq 23559, length 44
IP 192.168.0.110 > 192.168.1.73: ICMP echo request, id 12293, seq 17419, length 44
IP 192.168.0.110 > 192.168.1.74: ICMP echo request, id 12293, seq 11279, length 44
IP 192.168.0.110 > 192.168.1.74: ICMP echo request, id 12293, seq 5139, length 44
IP 192.168.0.110 > 192.168.1.75: ICMP echo request, id 12293, seq 64534, length 44
IP 192.168.0.110 > 192.168.1.75: ICMP echo request, id 12293, seq 58394, length 44
IP 192.168.0.110 > 192.168.1.76: ICMP echo request, id 12293, seq 52254, length 44
IP 192.168.0.110 > 192.168.1.76: ICMP echo request, id 12293, seq 46114, length 44
IP 192.168.0.110 > 192.168.1.77: ICMP echo request, id 12293, seq 39974, length 44
IP 192.168.0.110 > 192.168.1.77: ICMP echo request, id 12293, seq 33834, length 44
IP 192.168.0.110 > 192.168.1.78: ICMP echo request, id 12293, seq 27694, length 44
IP 192.168.0.110 > 192.168.1.78: ICMP echo request, id 12293, seq 21554, length 44
IP 192.168.0.110 > 192.168.1.79: ICMP echo request, id 12293, seq 15414, length 44
IP 192.168.0.110 > 192.168.1.79: ICMP echo request, id 12293, seq 9274, length 44
IP 192.168.0.110 > 192.168.1.80: ICMP echo request, id 12293, seq 3134, length 44
```

```
IP 192.168.0.110 > 192.168.1.80: ICMP echo request, id 12293, seq 62529, length 44
IP 192.168.0.110 > 192.168.1.81: ICMP echo request, id 12293, seq 56389, length 44
IP 192.168.0.110 > 192.168.1.81: ICMP echo request, id 12293, seq 50249, length 44
IP 192.168.0.110 > 192.168.1.82: ICMP echo request, id 12293, seq 44109, length 44
IP 192.168.0.110 > 192.168.1.82: ICMP echo request, id 12293, seq 37969, length 44
IP 192.168.0.110 > 192.168.1.83: ICMP echo request, id 12293, seq 31829, length 44
IP 192.168.0.110 > 192.168.1.83: ICMP echo request, id 12293, seq 25689, length 44
IP 192.168.0.110 > 192.168.1.84: ICMP echo request, id 12293, seq 19549, length 44
IP 192.168.0.110 > 192.168.1.84: ICMP echo request, id 12293, seq 13409, length 44
IP 192.168.0.110 > 192.168.1.85: ICMP echo request, id 12293, seq 7269, length 44
IP 192.168.0.110 > 192.168.1.85: ICMP echo request, id 12293, seq 1129, length 44
IP 192.168.0.110 > 192.168.1.86: ICMP echo request, id 12293, seq 60524, length 44
IP 192.168.0.110 > 192.168.1.86: ICMP echo request, id 12293, seq 54384, length 44
IP 192.168.0.110 > 192.168.1.87: ICMP echo request, id 12293, seq 48244, length 44
IP 192.168.0.110 > 192.168.1.87: ICMP echo request, id 12293, seq 42104, length 44
IP 192.168.0.110 > 192.168.1.88: ICMP echo request, id 12293, seq 35964, length 44
IP 192.168.0.110 > 192.168.1.88: ICMP echo request, id 12293, seq 29824, length 44
IP 192.168.0.110 > 192.168.1.89: ICMP echo request, id 12293, seq 23684, length 44
IP 192.168.0.110 > 192.168.1.89: ICMP echo request, id 12293, seq 17544, length 44
IP 192.168.0.110 > 192.168.1.90: ICMP echo request, id 12293, seq 11404, length 44
IP 192.168.0.110 > 192.168.1.90: ICMP echo request, id 12293, seq 5264, length 44
IP 192.168.0.110 > 192.168.1.91: ICMP echo request, id 12293, seq 64659, length 44
IP 192.168.0.110 > 192.168.1.91: ICMP echo request, id 12293, seq 58519, length 44
IP 192.168.0.110 > 192.168.1.92: ICMP echo request, id 12293, seq 52379, length 44
IP 192.168.0.110 > 192.168.1.92: ICMP echo request, id 12293, seq 46239, length 44
IP 192.168.0.110 > 192.168.1.93: ICMP echo request, id 12293, seq 40099, length 44
IP 192.168.0.110 > 192.168.1.93: ICMP echo request, id 12293, seq 33959, length 44
IP 192.168.0.110 > 192.168.1.94: ICMP echo request, id 12293, seq 27819, length 44
IP 192.168.0.110 > 192.168.1.94: ICMP echo request, id 12293, seq 21679, length 44
IP 192.168.0.110 > 192.168.1.95: ICMP echo request, id 12293, seq 15539, length 44
IP 192.168.0.110 > 192.168.1.95: ICMP echo request, id 12293, seq 9399, length 44
IP 192.168.0.110 > 192.168.1.96: ICMP echo request, id 12293, seq 3259, length 44
IP 192.168.0.110 > 192.168.1.96: ICMP echo request, id 12293, seq 62654, length 44
IP 192.168.0.110 > 192.168.1.97: ICMP echo request, id 12293, seq 56514, length 44
IP 192.168.0.110 > 192.168.1.97: ICMP echo request, id 12293, seq 50374, length 44
IP 192.168.0.110 > 192.168.1.98: ICMP echo request, id 12293, seq 44234, length 44
IP 192.168.0.110 > 192.168.1.98: ICMP echo request, id 12293, seq 38094, length 44
IP 192.168.0.110 > 192.168.1.99: ICMP echo request, id 12293, seq 31954, length 44
IP 192.168.0.110 > 192.168.1.99: ICMP echo request, id 12293, seq 25814, length 44
IP 192.168.0.110 > 192.168.1.100: ICMP echo request, id 12293, seq 19674, length 44
IP 192.168.0.110 > 192.168.1.100: ICMP echo request, id 12293, seq 13534, length 44
IP 192.168.0.110 > 192.168.1.101: ICMP echo request, id 12293, seq 7394, length 44
IP 192.168.0.110 > 192.168.1.101: ICMP echo request, id 12293, seq 1254, length 44
IP 192.168.0.110 > 192.168.1.102: ICMP echo request, id 12293, seq 60649, length 44
IP 192.168.0.110 > 192.168.1.102: ICMP echo request, id 12293, seq 54509, length 44
IP 192.168.0.110 > 192.168.1.103: ICMP echo request, id 12293, seq 48369, length 44
IP 192.168.0.110 > 192.168.1.103: ICMP echo request, id 12293, seq 42229, length 44
IP 192.168.0.110 > 192.168.1.104: ICMP echo request, id 12293, seq 36089, length 44
IP 192.168.0.110 > 192.168.1.104: ICMP echo request, id 12293, seq 29949, length 44
IP 192.168.0.110 > 192.168.1.105: ICMP echo request, id 12293, seq 23553, length 44
IP 192.168.0.110 > 192.168.1.105: ICMP echo request, id 12293, seq 17413, length 44
IP 192.168.0.110 > 192.168.1.106: ICMP echo request, id 12293, seq 11273, length 44
IP 192.168.0.110 > 192.168.1.106: ICMP echo request, id 12293, seq 5133, length 44
IP 192.168.0.110 > 192.168.1.107: ICMP echo request, id 12293, seq 64528, length 44
IP 192.168.0.110 > 192.168.1.107: ICMP echo request, id 12293, seq 58388, length 44
IP 192.168.0.110 > 192.168.1.108: ICMP echo request, id 12293, seq 52248, length 44
IP 192.168.0.110 > 192.168.1.108: ICMP echo request, id 12293, seq 46108, length 44
IP 192.168.0.110 > 192.168.1.109: ICMP echo request, id 12293, seq 39968, length 44
IP 192.168.0.110 > 192.168.1.109: ICMP echo request, id 12293, seq 33828, length 44
IP 192.168.0.110 > 192.168.1.110: ICMP echo request, id 12293, seq 27688, length 44
IP 192.168.0.110 > 192.168.1.110: ICMP echo request, id 12293, seq 21548, length 44
IP 192.168.0.110 > 192.168.1.111: ICMP echo request, id 12293, seq 15408, length 44
IP 192.168.0.110 > 192.168.1.111: ICMP echo request, id 12293, seq 9268, length 44
IP 192.168.0.110 > 192.168.1.112: ICMP echo request, id 12293, seq 3128, length 44
IP 192.168.0.110 > 192.168.1.112: ICMP echo request, id 12293, seq 62523, length 44
IP 192.168.0.110 > 192.168.1.113: ICMP echo request, id 12293, seq 56383, length 44
IP 192.168.0.110 > 192.168.1.113: ICMP echo request, id 12293, seq 50243, length 44
IP 192.168.0.110 > 192.168.1.114: ICMP echo request, id 12293, seq 44103, length 44
IP 192.168.0.110 > 192.168.1.114: ICMP echo request, id 12293, seq 37963, length 44
IP 192.168.0.110 > 192.168.1.115: ICMP echo request, id 12293, seq 31823, length 44
IP 192.168.0.110 > 192.168.1.115: ICMP echo request, id 12293, seq 25683, length 44
IP 192.168.0.110 > 192.168.1.116: ICMP echo request, id 12293, seq 19543, length 44
IP 192.168.0.110 > 192.168.1.116: ICMP echo request, id 12293, seq 13403, length 44
IP 192.168.0.110 > 192.168.1.117: ICMP echo request, id 12293, seq 7263, length 44
IP 192.168.0.110 > 192.168.1.117: ICMP echo request, id 12293, seq 1123, length 44
IP 192.168.0.110 > 192.168.1.118: ICMP echo request, id 12293, seq 60518, length 44
IP 192.168.0.110 > 192.168.1.118: ICMP echo request, id 12293, seq 54378, length 44
IP 192.168.0.110 > 192.168.1.119: ICMP echo request, id 12293, seq 48238, length 44
IP 192.168.0.110 > 192.168.1.119: ICMP echo request, id 12293, seq 42098, length 44
IP 192.168.0.110 > 192.168.1.120: ICMP echo request, id 12293, seq 35958, length 44
IP 192.168.0.110 > 192.168.1.120: ICMP echo request, id 12293, seq 29818, length 44
IP 192.168.0.110 > 192.168.1.121: ICMP echo request, id 12293, seq 23678, length 44
IP 192.168.0.110 > 192.168.1.121: ICMP echo request, id 12293, seq 17538, length 44
IP 192.168.0.110 > 192.168.1.122: ICMP echo request, id 12293, seq 11398, length 44
IP 192.168.0.110 > 192.168.1.122: ICMP echo request, id 12293, seq 5258, length 44
IP 192.168.0.110 > 192.168.1.123: ICMP echo request, id 12293, seq 64653, length 44
IP 192.168.0.110 > 192.168.1.123: ICMP echo request, id 12293, seq 58513, length 44
IP 192.168.0.110 > 192.168.1.124: ICMP echo request, id 12293, seq 52373, length 44
```

```
IP 192.168.0.110 > 192.168.1.124: ICMP echo request, id 12293, seq 46233, length 44
IP 192.168.0.110 > 192.168.1.125: ICMP echo request, id 12293, seq 40093, length 44
IP 192.168.0.110 > 192.168.1.125: ICMP echo request, id 12293, seq 33953, length 44
IP 192.168.0.110 > 192.168.1.126: ICMP echo request, id 12293, seq 27813, length 44
IP 192.168.0.110 > 192.168.1.126: ICMP echo request, id 12293, seq 21673, length 44
IP 192.168.0.110 > 192.168.1.127: ICMP echo request, id 12293, seq 15533, length 44
IP 192.168.0.110 > 192.168.1.127: ICMP echo request, id 12293, seq 9393, length 44
IP 192.168.0.110 > 192.168.1.128: ICMP echo request, id 12293, seq 3253, length 44
IP 192.168.0.110 > 192.168.1.128: ICMP echo request, id 12293, seq 62648, length 44
IP 192.168.0.110 > 192.168.1.129: ICMP echo request, id 12293, seq 56508, length 44
IP 192.168.0.110 > 192.168.1.129: ICMP echo request, id 12293, seq 50368, length 44
IP 192.168.0.110 > 192.168.1.130: ICMP echo request, id 12293, seq 44228, length 44
IP 192.168.0.110 > 192.168.1.130: ICMP echo request, id 12293, seq 38088, length 44
IP 192.168.0.110 > 192.168.1.131: ICMP echo request, id 12293, seq 31948, length 44
IP 192.168.0.110 > 192.168.1.131: ICMP echo request, id 12293, seq 25808, length 44
IP 192.168.0.110 > 192.168.1.132: ICMP echo request, id 12293, seq 19668, length 44
IP 192.168.0.110 > 192.168.1.132: ICMP echo request, id 12293, seq 13528, length 44
IP 192.168.0.110 > 192.168.1.133: ICMP echo request, id 12293, seq 7388, length 44
IP 192.168.0.110 > 192.168.1.133: ICMP echo request, id 12293, seq 1248, length 44
IP 192.168.0.110 > 192.168.1.134: ICMP echo request, id 12293, seq 60643, length 44
IP 192.168.0.110 > 192.168.1.134: ICMP echo request, id 12293, seq 54503, length 44
IP 192.168.0.110 > 192.168.1.135: ICMP echo request, id 12293, seq 48363, length 44
IP 192.168.0.110 > 192.168.1.135: ICMP echo request, id 12293, seq 42223, length 44
IP 192.168.0.110 > 192.168.1.136: ICMP echo request, id 12293, seq 36083, length 44
IP 192.168.0.110 > 192.168.1.136: ICMP echo request, id 12293, seq 29943, length 44
IP 192.168.0.110 > 192.168.1.137: ICMP echo request, id 12293, seq 23803, length 44
IP 192.168.0.110 > 192.168.1.137: ICMP echo request, id 12293, seq 17663, length 44
IP 192.168.0.110 > 192.168.1.138: ICMP echo request, id 12293, seq 11267, length 44
IP 192.168.0.110 > 192.168.1.138: ICMP echo request, id 12293, seq 5127, length 44
IP 192.168.0.110 > 192.168.1.139: ICMP echo request, id 12293, seq 64522, length 44
IP 192.168.0.110 > 192.168.1.139: ICMP echo request, id 12293, seq 58382, length 44
IP 192.168.0.110 > 192.168.1.140: ICMP echo request, id 12293, seq 52242, length 44
IP 192.168.0.110 > 192.168.1.140: ICMP echo request, id 12293, seq 46102, length 44
IP 192.168.0.110 > 192.168.1.141: ICMP echo request, id 12293, seq 39962, length 44
IP 192.168.0.110 > 192.168.1.141: ICMP echo request, id 12293, seq 33822, length 44
IP 192.168.0.110 > 192.168.1.142: ICMP echo request, id 12293, seq 27682, length 44
IP 192.168.0.110 > 192.168.1.142: ICMP echo request, id 12293, seq 21542, length 44
IP 192.168.0.110 > 192.168.1.143: ICMP echo request, id 12293, seq 15402, length 44
IP 192.168.0.110 > 192.168.1.143: ICMP echo request, id 12293, seq 9262, length 44
IP 192.168.0.110 > 192.168.1.144: ICMP echo request, id 12293, seq 3122, length 44
IP 192.168.0.110 > 192.168.1.144: ICMP echo request, id 12293, seq 62517, length 44
IP 192.168.0.110 > 192.168.1.145: ICMP echo request, id 12293, seq 56377, length 44
IP 192.168.0.110 > 192.168.1.145: ICMP echo request, id 12293, seq 50237, length 44
IP 192.168.0.110 > 192.168.1.146: ICMP echo request, id 12293, seq 44097, length 44
IP 192.168.0.110 > 192.168.1.146: ICMP echo request, id 12293, seq 37957, length 44
IP 192.168.0.110 > 192.168.1.147: ICMP echo request, id 12293, seq 31817, length 44
IP 192.168.0.110 > 192.168.1.147: ICMP echo request, id 12293, seq 25677, length 44
IP 192.168.0.110 > 192.168.1.148: ICMP echo request, id 12293, seq 19537, length 44
IP 192.168.0.110 > 192.168.1.148: ICMP echo request, id 12293, seq 13397, length 44
IP 192.168.0.110 > 192.168.1.149: ICMP echo request, id 12293, seq 7257, length 44
IP 192.168.0.110 > 192.168.1.149: ICMP echo request, id 12293, seq 1117, length 44
IP 192.168.0.110 > 192.168.1.150: ICMP echo request, id 12293, seq 60512, length 44
IP 192.168.0.110 > 192.168.1.150: ICMP echo request, id 12293, seq 54372, length 44
IP 192.168.0.110 > 192.168.1.151: ICMP echo request, id 12293, seq 48232, length 44
IP 192.168.0.110 > 192.168.1.151: ICMP echo request, id 12293, seq 42092, length 44
IP 192.168.0.110 > 192.168.1.152: ICMP echo request, id 12293, seq 35952, length 44
IP 192.168.0.110 > 192.168.1.152: ICMP echo request, id 12293, seq 29812, length 44
IP 192.168.0.110 > 192.168.1.153: ICMP echo request, id 12293, seq 23672, length 44
IP 192.168.0.110 > 192.168.1.153: ICMP echo request, id 12293, seq 17532, length 44
IP 192.168.0.110 > 192.168.1.154: ICMP echo request, id 12293, seq 11392, length 44
IP 192.168.0.110 > 192.168.1.154: ICMP echo request, id 12293, seq 5252, length 44
IP 192.168.0.110 > 192.168.1.155: ICMP echo request, id 12293, seq 64647, length 44
IP 192.168.0.110 > 192.168.1.155: ICMP echo request, id 12293, seq 58507, length 44
IP 192.168.0.110 > 192.168.1.156: ICMP echo request, id 12293, seq 52367, length 44
IP 192.168.0.110 > 192.168.1.156: ICMP echo request, id 12293, seq 46227, length 44
IP 192.168.0.110 > 192.168.1.157: ICMP echo request, id 12293, seq 40087, length 44
IP 192.168.0.110 > 192.168.1.157: ICMP echo request, id 12293, seq 33947, length 44
IP 192.168.0.110 > 192.168.1.158: ICMP echo request, id 12293, seq 27807, length 44
IP 192.168.0.110 > 192.168.1.158: ICMP echo request, id 12293, seq 21667, length 44
IP 192.168.0.110 > 192.168.1.159: ICMP echo request, id 12293, seq 15527, length 44
IP 192.168.0.110 > 192.168.1.159: ICMP echo request, id 12293, seq 9387, length 44
IP 192.168.0.110 > 192.168.1.160: ICMP echo request, id 12293, seq 3247, length 44
IP 192.168.0.110 > 192.168.1.160: ICMP echo request, id 12293, seq 62642, length 44
IP 192.168.0.110 > 192.168.1.161: ICMP echo request, id 12293, seq 56502, length 44
IP 192.168.0.110 > 192.168.1.161: ICMP echo request, id 12293, seq 50362, length 44
IP 192.168.0.110 > 192.168.1.162: ICMP echo request, id 12293, seq 44222, length 44
IP 192.168.0.110 > 192.168.1.162: ICMP echo request, id 12293, seq 38082, length 44
IP 192.168.0.110 > 192.168.1.163: ICMP echo request, id 12293, seq 31942, length 44
IP 192.168.0.110 > 192.168.1.163: ICMP echo request, id 12293, seq 25802, length 44
IP 192.168.0.110 > 192.168.1.164: ICMP echo request, id 12293, seq 19662, length 44
IP 192.168.0.110 > 192.168.1.164: ICMP echo request, id 12293, seq 13522, length 44
IP 192.168.0.110 > 192.168.1.165: ICMP echo request, id 12293, seq 7382, length 44
IP 192.168.0.110 > 192.168.1.165: ICMP echo request, id 12293, seq 1242, length 44
IP 192.168.0.110 > 192.168.1.166: ICMP echo request, id 12293, seq 60637, length 44
IP 192.168.0.110 > 192.168.1.166: ICMP echo request, id 12293, seq 54497, length 44
IP 192.168.0.110 > 192.168.1.167: ICMP echo request, id 12293, seq 48357, length 44
IP 192.168.0.110 > 192.168.1.167: ICMP echo request, id 12293, seq 42217, length 44
IP 192.168.0.110 > 192.168.1.168: ICMP echo request, id 12293, seq 36077, length 44
```

```
IP 192.168.0.110 > 192.168.1.168: ICMP echo request, id 12293, seq 29937, length 44
IP 192.168.0.110 > 192.168.1.169: ICMP echo request, id 12293, seq 23797, length 44
IP 192.168.0.110 > 192.168.1.169: ICMP echo request, id 12293, seq 17657, length 44
IP 192.168.0.110 > 192.168.1.170: ICMP echo request, id 12293, seq 11517, length 44
IP 192.168.0.110 > 192.168.1.170: ICMP echo request, id 12293, seq 5121, length 44
IP 192.168.0.110 > 192.168.1.171: ICMP echo request, id 12293, seq 64516, length 44
IP 192.168.0.110 > 192.168.1.171: ICMP echo request, id 12293, seq 58376, length 44
IP 192.168.0.110 > 192.168.1.172: ICMP echo request, id 12293, seq 52236, length 44
IP 192.168.0.110 > 192.168.1.172: ICMP echo request, id 12293, seq 46096, length 44
IP 192.168.0.110 > 192.168.1.173: ICMP echo request, id 12293, seq 39956, length 44
IP 192.168.0.110 > 192.168.1.173: ICMP echo request, id 12293, seq 33816, length 44
IP 192.168.0.110 > 192.168.1.174: ICMP echo request, id 12293, seq 27676, length 44
IP 192.168.0.110 > 192.168.1.174: ICMP echo request, id 12293, seq 21536, length 44
IP 192.168.0.110 > 192.168.1.175: ICMP echo request, id 12293, seq 15396, length 44
IP 192.168.0.110 > 192.168.1.175: ICMP echo request, id 12293, seq 9256, length 44
IP 192.168.0.110 > 192.168.1.176: ICMP echo request, id 12293, seq 3116, length 44
IP 192.168.0.110 > 192.168.1.176: ICMP echo request, id 12293, seq 62511, length 44
IP 192.168.0.110 > 192.168.1.177: ICMP echo request, id 12293, seq 56371, length 44
IP 192.168.0.110 > 192.168.1.177: ICMP echo request, id 12293, seq 50231, length 44
IP 192.168.0.110 > 192.168.1.178: ICMP echo request, id 12293, seq 44091, length 44
IP 192.168.0.110 > 192.168.1.178: ICMP echo request, id 12293, seq 37951, length 44
IP 192.168.0.110 > 192.168.1.179: ICMP echo request, id 12293, seq 31811, length 44
IP 192.168.0.110 > 192.168.1.179: ICMP echo request, id 12293, seq 25671, length 44
IP 192.168.0.110 > 192.168.1.180: ICMP echo request, id 12293, seq 19531, length 44
IP 192.168.0.110 > 192.168.1.180: ICMP echo request, id 12293, seq 13391, length 44
IP 192.168.0.110 > 192.168.1.181: ICMP echo request, id 12293, seq 7251, length 44
IP 192.168.0.110 > 192.168.1.181: ICMP echo request, id 12293, seq 1111, length 44
IP 192.168.0.110 > 192.168.1.182: ICMP echo request, id 12293, seq 60506, length 44
IP 192.168.0.110 > 192.168.1.182: ICMP echo request, id 12293, seq 54366, length 44
IP 192.168.0.110 > 192.168.1.183: ICMP echo request, id 12293, seq 48226, length 44
IP 192.168.0.110 > 192.168.1.183: ICMP echo request, id 12293, seq 42086, length 44
IP 192.168.0.110 > 192.168.1.184: ICMP echo request, id 12293, seq 35946, length 44
IP 192.168.0.110 > 192.168.1.184: ICMP echo request, id 12293, seq 29806, length 44
IP 192.168.0.110 > 192.168.1.185: ICMP echo request, id 12293, seq 23666, length 44
IP 192.168.0.110 > 192.168.1.185: ICMP echo request, id 12293, seq 17526, length 44
IP 192.168.0.110 > 192.168.1.186: ICMP echo request, id 12293, seq 11386, length 44
IP 192.168.0.110 > 192.168.1.186: ICMP echo request, id 12293, seq 5246, length 44
IP 192.168.0.110 > 192.168.1.187: ICMP echo request, id 12293, seq 64641, length 44
IP 192.168.0.110 > 192.168.1.187: ICMP echo request, id 12293, seq 58501, length 44
IP 192.168.0.110 > 192.168.1.188: ICMP echo request, id 12293, seq 52361, length 44
IP 192.168.0.110 > 192.168.1.188: ICMP echo request, id 12293, seq 46221, length 44
IP 192.168.0.110 > 192.168.1.189: ICMP echo request, id 12293, seq 40081, length 44
IP 192.168.0.110 > 192.168.1.189: ICMP echo request, id 12293, seq 33941, length 44
IP 192.168.0.110 > 192.168.1.190: ICMP echo request, id 12293, seq 27801, length 44
IP 192.168.0.110 > 192.168.1.190: ICMP echo request, id 12293, seq 21661, length 44
IP 192.168.0.110 > 192.168.1.191: ICMP echo request, id 12293, seq 15521, length 44
IP 192.168.0.110 > 192.168.1.191: ICMP echo request, id 12293, seq 9381, length 44
IP 192.168.0.110 > 192.168.1.192: ICMP echo request, id 12293, seq 3241, length 44
IP 192.168.0.110 > 192.168.1.192: ICMP echo request, id 12293, seq 62636, length 44
IP 192.168.0.110 > 192.168.1.193: ICMP echo request, id 12293, seq 56496, length 44
IP 192.168.0.110 > 192.168.1.193: ICMP echo request, id 12293, seq 50356, length 44
IP 192.168.0.110 > 192.168.1.194: ICMP echo request, id 12293, seq 44216, length 44
IP 192.168.0.110 > 192.168.1.194: ICMP echo request, id 12293, seq 38076, length 44
IP 192.168.0.110 > 192.168.1.195: ICMP echo request, id 12293, seq 31936, length 44
IP 192.168.0.110 > 192.168.1.195: ICMP echo request, id 12293, seq 25796, length 44
IP 192.168.0.110 > 192.168.1.196: ICMP echo request, id 12293, seq 19656, length 44
IP 192.168.0.110 > 192.168.1.196: ICMP echo request, id 12293, seq 13516, length 44
IP 192.168.0.110 > 192.168.1.197: ICMP echo request, id 12293, seq 7376, length 44
IP 192.168.0.110 > 192.168.1.197: ICMP echo request, id 12293, seq 1236, length 44
IP 192.168.0.110 > 192.168.1.198: ICMP echo request, id 12293, seq 60631, length 44
IP 192.168.0.110 > 192.168.1.198: ICMP echo request, id 12293, seq 54491, length 44
IP 192.168.0.110 > 192.168.1.199: ICMP echo request, id 12293, seq 48351, length 44
IP 192.168.0.110 > 192.168.1.199: ICMP echo request, id 12293, seq 42211, length 44
IP 192.168.0.110 > 192.168.1.200: ICMP echo request, id 12293, seq 36071, length 44
IP 192.168.0.110 > 192.168.1.200: ICMP echo request, id 12293, seq 29931, length 44
IP 192.168.0.110 > 192.168.1.201: ICMP echo request, id 12293, seq 23791, length 44
IP 192.168.0.110 > 192.168.1.201: ICMP echo request, id 12293, seq 17651, length 44
IP 192.168.0.110 > 192.168.1.202: ICMP echo request, id 12293, seq 11511, length 44
IP 192.168.0.110 > 192.168.1.202: ICMP echo request, id 12293, seq 5371, length 44
IP 192.168.0.110 > 192.168.1.203: ICMP echo request, id 12293, seq 64766, length 44
IP 192.168.0.110 > 192.168.1.203: ICMP echo request, id 12293, seq 58370, length 44
IP 192.168.0.110 > 192.168.1.204: ICMP echo request, id 12293, seq 52230, length 44
IP 192.168.0.110 > 192.168.1.204: ICMP echo request, id 12293, seq 46090, length 44
IP 192.168.0.110 > 192.168.1.205: ICMP echo request, id 12293, seq 39950, length 44
IP 192.168.0.110 > 192.168.1.205: ICMP echo request, id 12293, seq 33810, length 44
IP 192.168.0.110 > 192.168.1.206: ICMP echo request, id 12293, seq 27670, length 44
IP 192.168.0.110 > 192.168.1.206: ICMP echo request, id 12293, seq 21530, length 44
IP 192.168.0.110 > 192.168.1.207: ICMP echo request, id 12293, seq 15390, length 44
IP 192.168.0.110 > 192.168.1.207: ICMP echo request, id 12293, seq 9250, length 44
IP 192.168.0.110 > 192.168.1.208: ICMP echo request, id 12293, seq 3110, length 44
IP 192.168.0.110 > 192.168.1.208: ICMP echo request, id 12293, seq 62505, length 44
IP 192.168.0.110 > 192.168.1.209: ICMP echo request, id 12293, seq 56365, length 44
IP 192.168.0.110 > 192.168.1.209: ICMP echo request, id 12293, seq 50225, length 44
IP 192.168.0.110 > 192.168.1.210: ICMP echo request, id 12293, seq 44085, length 44
IP 192.168.0.110 > 192.168.1.210: ICMP echo request, id 12293, seq 37945, length 44
IP 192.168.0.110 > 192.168.1.211: ICMP echo request, id 12293, seq 47677, length 44
IP 192.168.0.110 > 192.168.1.211: ICMP echo request, id 12293, seq 41537, length 44
IP 192.168.0.110 > 192.168.1.212: ICMP echo request, id 12293, seq 35397, length 44
```

```
IP 192.168.0.110 > 192.168.1.212: ICMP echo request, id 12293, seq 29257, length 44
IP 192.168.0.110 > 192.168.1.213: ICMP echo request, id 12293, seq 23117, length 44
IP 192.168.0.110 > 192.168.1.213: ICMP echo request, id 12293, seq 16977, length 44
IP 192.168.0.110 > 192.168.1.214: ICMP echo request, id 12293, seq 10837, length 44
IP 192.168.0.110 > 192.168.1.214: ICMP echo request, id 12293, seq 4697, length 44
IP 192.168.0.110 > 192.168.1.215: ICMP echo request, id 12293, seq 64092, length 44
IP 192.168.0.110 > 192.168.1.215: ICMP echo request, id 12293, seq 57952, length 44
IP 192.168.0.110 > 192.168.1.216: ICMP echo request, id 12293, seq 6245, length 44
IP 192.168.0.110 > 192.168.1.216: ICMP echo request, id 12293, seq 105, length 44
IP 192.168.0.110 > 192.168.1.217: ICMP echo request, id 12293, seq 59500, length 44
IP 192.168.0.110 > 192.168.1.217: ICMP echo request, id 12293, seq 53360, length 44

>> Advanced Intrusion Detection Environment <<
Start timestamp: 2012-03-20 19:32:24

Summary:
  Total number of files:        10176
  Added files:                  11
  Removed files:                0
  Changed files:                50


---------------------------------------------------
Added files:
---------------------------------------------------

added: /mnt/images/WINDOWS/Prefetch/RUNDLL32.EXE-354F49E0.pf
added: /mnt/images/WINDOWS/Prefetch/RUNDLL32.EXE-3C36C47F.pf
added: /mnt/images/WINDOWS/Prefetch/TASKMGR.EXE-20256C55.pf
added: /mnt/images/WINDOWS/Prefetch/MSPAINT.EXE-11CBB631.pf
added: /mnt/images/WINDOWS/Prefetch/OFFDIAG.EXE-120B291F.pf
added: /mnt/images/WINDOWS/Prefetch/CLVIEW.EXE-1013077A.pf
added: /mnt/images/WINDOWS/Prefetch/DW20.EXE-22C39A55.pf
added: /mnt/images/WINDOWS/Prefetch/EXCEL.EXE-34CB65E9.pf
added: /mnt/images/WINDOWS/system32/c_20178.nls
added: /mnt/images/WINDOWS/Temp/10d81856.rar
added: /mnt/images/WINDOWS/Temp/5c30765f.rar

---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /mnt/images/WINDOWS/Debug/UserMode/userenv.log
changed: /mnt/images/WINDOWS/Prefetch/101142C1.EXE-26610E3C.pf
changed: /mnt/images/WINDOWS/Prefetch/CAPTUREBAT.EXE-056A1A48.pf
changed: /mnt/images/WINDOWS/Prefetch/RUNDLL32.EXE-451FC2C0.pf
changed: /mnt/images/WINDOWS/Prefetch/SVCHOST.EXE-3530F672.pf
changed: /mnt/images/WINDOWS/Prefetch/LOGONUI.EXE-0AF22957.pf
changed: /mnt/images/WINDOWS/Prefetch/NOTEPAD.EXE-336351A9.pf
changed: /mnt/images/WINDOWS/Prefetch/NTOSBOOT-B00DFAAD.pf
changed: /mnt/images/WINDOWS/Prefetch/EXPLORER.EXE-082F38A9.pf
changed: /mnt/images/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
changed: /mnt/images/WINDOWS/Prefetch/CONIME.EXE-13EEEA1A.pf
changed: /mnt/images/WINDOWS/Prefetch/DD.EXE-065AC9AE.pf
changed: /mnt/images/WINDOWS/Prefetch/VERCLSID.EXE-3667BD89.pf
changed: /mnt/images/WINDOWS/Prefetch/WSCNTFY.EXE-1B24F5EB.pf
changed: /mnt/images/WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf
changed: /mnt/images/WINDOWS/SoftwareDistribution/DataStore/DataStore.edb
changed: /mnt/images/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk
changed: /mnt/images/WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log
changed: /mnt/images/WINDOWS/system32/wbem/Repository/FS/INDEX.BTR
changed: /mnt/images/WINDOWS/system32/wbem/Repository/FS/INDEX.MAP
changed: /mnt/images/WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP
changed: /mnt/images/WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP
changed: /mnt/images/WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA
changed: /mnt/images/WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP
changed: /mnt/images/WINDOWS/system32/wbem/Logs/wbemcore.log
changed: /mnt/images/WINDOWS/system32/wbem/Logs/wbemess.log
changed: /mnt/images/WINDOWS/system32/wbem/Logs/wmiprov.log
changed: /mnt/images/WINDOWS/system32/config/AppEvent.Evt
changed: /mnt/images/WINDOWS/system32/config/default
changed: /mnt/images/WINDOWS/system32/config/default.LOG
changed: /mnt/images/WINDOWS/system32/config/ODiag.evt
changed: /mnt/images/WINDOWS/system32/config/OSession.evt
changed: /mnt/images/WINDOWS/system32/config/SAM
changed: /mnt/images/WINDOWS/system32/config/SAM.LOG
changed: /mnt/images/WINDOWS/system32/config/SECURITY
changed: /mnt/images/WINDOWS/system32/config/SECURITY.LOG
changed: /mnt/images/WINDOWS/system32/config/software
changed: /mnt/images/WINDOWS/system32/config/software.LOG
changed: /mnt/images/WINDOWS/system32/config/SysEvent.Evt
changed: /mnt/images/WINDOWS/system32/config/system
changed: /mnt/images/WINDOWS/system32/config/system.LOG
changed: /mnt/images/WINDOWS/system32/drivers/tcpip.sys
changed: /mnt/images/WINDOWS/system32/CatRoot2/edb.chk
changed: /mnt/images/WINDOWS/system32/CatRoot2/edb.log
changed: /mnt/images/WINDOWS/system32/CatRoot2/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/catdb
changed: /mnt/images/WINDOWS/SchedLgU.Txt
```

changed: /mnt/images/WINDOWS/setupapi.log
changed: /mnt/images/WINDOWS/wiadebug.log
changed: /mnt/images/WINDOWS/wiaservc.log
changed: /mnt/images/WINDOWS/WindowsUpdate.log

Offical Web: http:://TWAN.ORG | Mail: TonTon@TWMAN.ORG
Cored By Truman 0.1, Developed By TonTon
臺灣惡意程式分析網+，抬丸郎+ - 分析報告 2012-03-15 版
Taiwan Malware Analysis Net+, TWMAN+ - Analysis Report