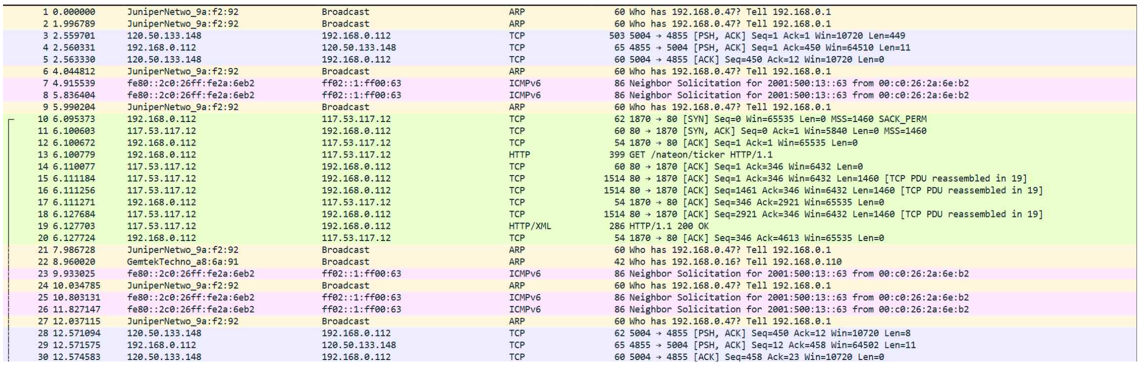


```
 1 0.000000    JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
 2 1.996789    JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
 3 2.559701    120.50.133.148              192.168.0.112      TCP        503 5004 → 4855 [PSH, ACK] Seq=1 Ack=1 Win=10720 Len=449
 4 2.560331    192.168.0.112               120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=1 Ack=450 Win=64510 Len=11
 5 2.563330    120.50.133.148              192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=450 Ack=12 Win=10720 Len=0
 6 4.044812    JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
 7 4.915539    fe80::2c0:26ff:fe2a:6eb2    ff02::1:ff00:63    ICMPv6      86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
 8 5.836404    fe80::2c0:26ff:fe2a:6eb2    ff02::1:ff00:63    ICMPv6      86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
 9 5.990204    JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
10 6.095373    192.168.0.112               117.53.117.12      TCP         62 1870 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
11 6.100603    117.53.117.12               192.168.0.112      TCP         60 80 → 1870 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
12 6.100672    192.168.0.112               117.53.117.12      TCP         54 1870 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
13 6.100779    192.168.0.112               117.53.117.12      HTTP       399 GET /nateon/ticker HTTP/1.1
14 6.110077    117.53.117.12               192.168.0.112      TCP         60 80 → 1870 [ACK] Seq=1 Ack=346 Win=6432 Len=0
15 6.111184    117.53.117.12               192.168.0.112      TCP       1514 80 → 1870 [ACK] Seq=1 Ack=346 Win=6432 Len=1460 [TCP PDU reassembled in 19]
16 6.111256    117.53.117.12               192.168.0.112      TCP       1514 80 → 1870 [ACK] Seq=1461 Ack=346 Win=6432 Len=1460 [TCP PDU reassembled in 19]
17 6.111271    192.168.0.112               117.53.117.12      TCP         54 1870 → 80 [ACK] Seq=346 Ack=2921 Win=65535 Len=0
18 6.127684    117.53.117.12               192.168.0.112      TCP       1514 80 → 1870 [ACK] Seq=2921 Ack=346 Win=6432 Len=1460 [TCP PDU reassembled in 19]
19 6.127703    117.53.117.12               192.168.0.112      HTTP/XML   286 HTTP/1.1 200 OK
20 6.127724    192.168.0.112               117.53.117.12      TCP         54 1870 → 80 [ACK] Seq=346 Ack=4613 Win=65535 Len=0
21 7.986728    JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
22 8.960020    GemtekTechno_a8:6a:91       Broadcast          ARP         42 Who has 192.168.0.16? Tell 192.168.0.110
23 9.933025    fe80::2c0:26ff:fe2a:6eb2    ff02::1:ff00:63    ICMPv6      86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
24 10.034785   JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
25 10.803131   fe80::2c0:26ff:fe2a:6eb2    ff02::1:ff00:63    ICMPv6      86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
26 11.827147   fe80::2c0:26ff:fe2a:6eb2    ff02::1:ff00:63    ICMPv6      86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
27 12.037115   JuniperNetwo_9a:f2:92       Broadcast          ARP         60 Who has 192.168.0.47? Tell 192.168.0.1
28 12.571094   120.50.133.148              192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=450 Ack=12 Win=10720 Len=8
29 12.571575   192.168.0.112               120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=12 Ack=458 Win=64502 Len=11
30 12.574583   120.50.133.148              192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=458 Ack=23 Win=10720 Len=0
```

ARP 요청
패킷 1, 2, 6, 9, 21, 22, 24, 27
MAC 주소 : 00:14:f6:9a:f2:92 IP : 192.168.0.1에서 지속적으로
192.168.0.47의 IP주소값을 가진 MAC주소를 찾고 있는 ARP메시지를 보내고 있음

패킷 3,4
출발지 IP : 120.50.133.148
목적지 IP : 192.168.0.112
TCP 연결이 시작 되었고 449바이트의 데이터가 전송하였고 PSH 플래그를 사용해 데이터를 즉시 처리하도록 지시

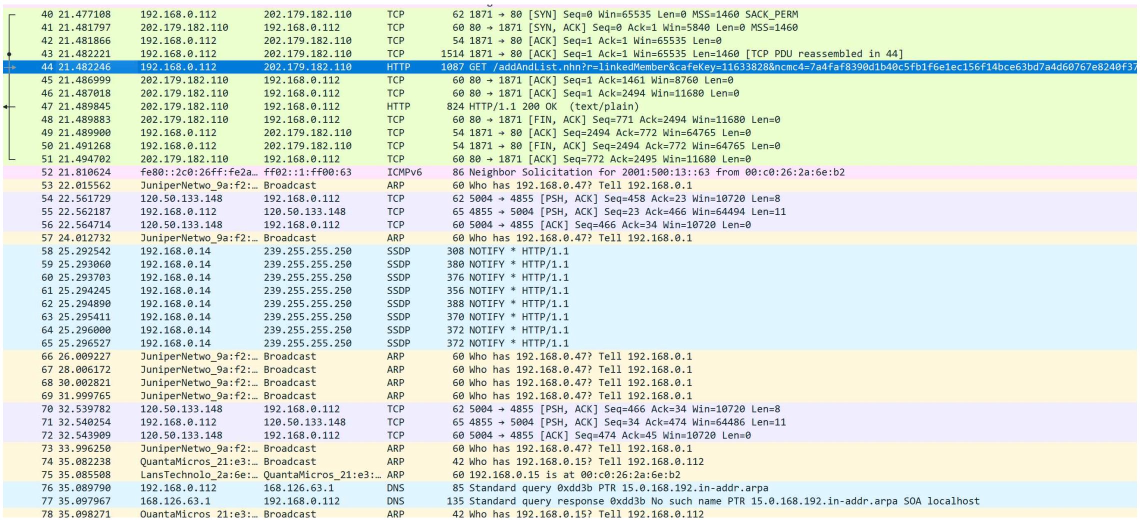
패킷 7,8
2001:500:13::63라는 IPv6주소에 대한 MAC 주소를 찾기 위해 fe80::2c0:26ff:fe2a:6eb2 장치가 Neighbor Solicitation을 보내는 상황

패킷 10 ~ 20
10 : SYN 플래그를 가진 패킷이 117.53.117.12에서 192.168.0.112로 전송.
11 : 192.168.0.112에서 117.53.117.12로 SYN-ACK 응답
12 : 117.53.117.12에서 다시 ACK 패킷을 보냄
13 : 클라이언트(192.168.0.112)가 서버(117.53.117.12)로 /nateon/ticker에 대한 데이터를 요청하는 패킷 TCP Segmet Len = 345 쿠기값 존재 get 요청
뉴스 메인 페이지 요청

14 : 117.53.117.12에서 192.168.0.112으로 get 요청에 대한 응답
15 ~ `8 : TCP PDU = (Protocol Data Unit) 패킷이 19에서 재조합되었다는뜻
17 : 16번 패킷에 대한 응답 15~16을 제대로 받았는지 응답하는 것 같음
19 : 13번 패킷에 대한 응답 200코드로 요청이 성공
http://newstkr.nate.com/nateon/ticker
20 : 서버에게 데이터를 잘 받았다고 응답
21 : 1,2번 패킷과 같음
22: 00:1a:73::a8:6a:91에서 192.168.0.16의 ip를 찾고 있다. 출발지 ip = 192.168.0.110

28 : 120.50.133.148 (5004)에서 192.168.0.112 (4855)로 즉시 데이터 처리 요청
27번에 대한응답이 맞는지 질문

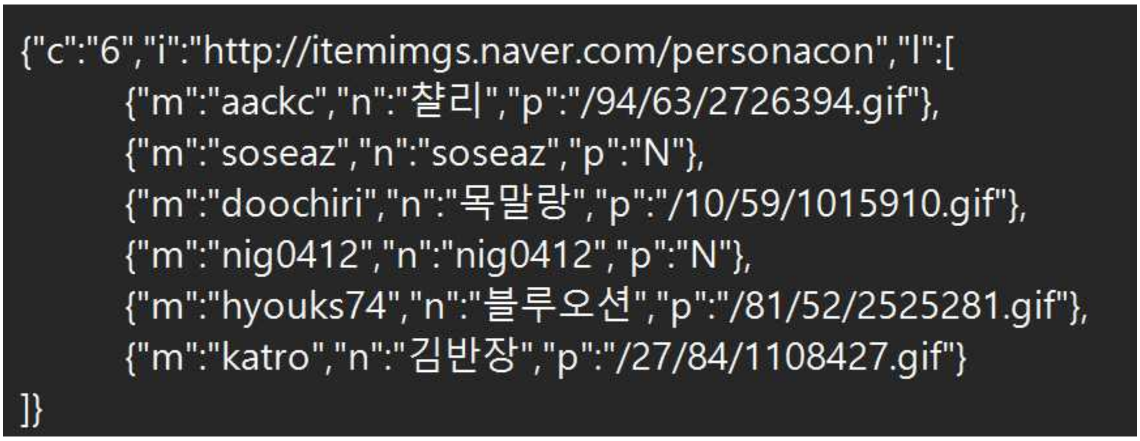
38 : 192.168.0.112(1870)에서 1174.53.117.12(80)의 응답 TCP연결을 리셋하는 RST 플래그와 ACK 응답이 설정된 패킷 TCP 연결을 종료 하거나 초기화 하려는 시도로 보임 윈도우 크기가 0인 것으로 보아 수신자가 더 이상 데이터를 받을 수 없다는 상태 인 것 같음
10번에서 연결된 연결 종료



```
40 21.477108   192.168.0.112        202.179.182.110      TCP      62 1871 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
41 21.481797   202.179.182.110      192.168.0.112        TCP      60 80 → 1871 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
42 21.481866   192.168.0.112        202.179.182.110      TCP      54 1871 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
43 21.482221   192.168.0.112        202.179.182.110      TCP    1514 1871 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=1460 [TCP PDU reassembled in 44]
44 21.482246   192.168.0.112        202.179.182.110      HTTP   1087 GET /addAndList.nhn?r=linkedMember&cafeKey=11633828&ncmc4=7a4faf8390d1b40c5fb1f6e1ec156f14bce63bd7a4d60767e8240f37
45 21.486999   202.179.182.110      192.168.0.112        TCP      60 80 → 1871 [ACK] Seq=1 Ack=1461 Win=8760 Len=0
46 21.487018   202.179.182.110      192.168.0.112        TCP      60 80 → 1871 [ACK] Seq=1 Ack=2494 Win=11680 Len=0
47 21.489845   202.179.182.110      192.168.0.112        HTTP    824 HTTP/1.1 200 OK  (text/plain)
48 21.489883   202.179.182.110      192.168.0.112        TCP      60 80 → 1871 [FIN, ACK] Seq=771 Ack=2494 Win=11680 Len=0
49 21.489900   192.168.0.112        202.179.182.110      TCP      54 1871 → 80 [ACK] Seq=2494 Ack=772 Win=64765 Len=0
50 21.491268   192.168.0.112        202.179.182.110      TCP      54 1871 → 80 [FIN, ACK] Seq=2494 Ack=772 Win=64765 Len=0
51 21.494702   202.179.182.110      192.168.0.112        TCP      60 80 → 1871 [ACK] Seq=772 Ack=2495 Win=11680 Len=0
52 21.810624   fe80::2c0:26ff:fe2a… ff02::1:ff00:63      ICMPv6   86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
53 22.015562   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
54 22.561729   120.50.133.148       192.168.0.112        TCP      62 5004 → 4855 [PSH, ACK] Seq=458 Ack=23 Win=10720 Len=8
55 22.562187   192.168.0.112        120.50.133.148       TCP      65 4855 → 5004 [PSH, ACK] Seq=23 Ack=466 Win=64494 Len=11
56 22.564714   120.50.133.148       192.168.0.112        TCP      60 5004 → 4855 [ACK] Seq=466 Ack=34 Win=10720 Len=0
57 24.012732   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
58 25.292542   192.168.0.14         239.255.255.250      SSDP    308 NOTIFY * HTTP/1.1
59 25.293060   192.168.0.14         239.255.255.250      SSDP    380 NOTIFY * HTTP/1.1
60 25.293703   192.168.0.14         239.255.255.250      SSDP    376 NOTIFY * HTTP/1.1
61 25.294245   192.168.0.14         239.255.255.250      SSDP    356 NOTIFY * HTTP/1.1
62 25.294890   192.168.0.14         239.255.255.250      SSDP    388 NOTIFY * HTTP/1.1
63 25.295411   192.168.0.14         239.255.255.250      SSDP    370 NOTIFY * HTTP/1.1
64 25.296000   192.168.0.14         239.255.255.250      SSDP    372 NOTIFY * HTTP/1.1
65 25.296527   192.168.0.14         239.255.255.250      SSDP    372 NOTIFY * HTTP/1.1
66 26.009227   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
67 28.006172   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
68 30.002821   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
69 31.999765   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
70 32.539782   120.50.133.148       192.168.0.112        TCP      62 5004 → 4855 [PSH, ACK] Seq=466 Ack=34 Win=10720 Len=8
71 32.540254   192.168.0.112        120.50.133.148       TCP      65 4855 → 5004 [PSH, ACK] Seq=34 Ack=474 Win=64486 Len=11
72 32.543909   120.50.133.148       192.168.0.112        TCP      60 5004 → 4855 [ACK] Seq=474 Ack=45 Win=10720 Len=0
73 33.996250   JuniperNetwo_9a:f2:… Broadcast            ARP      60 Who has 192.168.0.47? Tell 192.168.0.1
74 35.082238   QuantaMicros_21:e3:… Broadcast            ARP      42 Who has 192.168.0.15? Tell 192.168.0.112
75 35.085508   LansTechnolo_2a:6e:… QuantaMicros_21:e3:… ARP      60 192.168.0.15 is at 00:c0:26:2a:6e:b2
76 35.089790   192.168.0.112        168.126.63.1         DNS      85 Standard query 0xdd3b PTR 15.0.168.192.in-addr.arpa
77 35.097967   168.126.63.1         192.168.0.112        DNS     135 Standard query response 0xdd3b No such name PTR 15.0.168.192.in-addr.arpa SOA localhost
78 35.098271   QuantaMicros_21:e3:… Broadcast            ARP      42 Who has 192.168.0.15? Tell 192.168.0.112
```

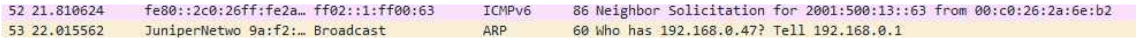
클라이언트(192.168.0.112)가 서버(202.179.182.110)의 HTTP 포트(80)에 접속을 시도하며 SYN 패킷을 보내서 핸드셰이크 완료됨.
MSS (Maximum Segment Size) 전송할 수 있는 최대 데이터 크기 1460바이트로 설정

패킷 44번
: 클라이언트 HTTP GET 요청을 보냄. txt 형식으로 확인 가능. 쿠키값 존재



```
{"c":"6","i":"http://itemimgs.naver.com/personacon","l":[
        {"m":"aackc","n":"챨리","p":"/94/63/2726394.gif"},
        {"m":"soseaz","n":"soseaz","p":"N"},
        {"m":"doochiri","n":"목말랑","p":"/10/59/1015910.gif"},
        {"m":"nig0412","n":"nig0412","p":"N"},
        {"m":"hyouks74","n":"블루오션","p":"/81/52/2525281.gif"},
        {"m":"katro","n":"김반장","p":"/27/84/1108427.gif"}
]}
```

이후 서버는 HTTP/1.1 200 OK 응답을 통해 요청을 정상 처리하고 클라이언트와 서버는 연결 정상적으로 종료.
사용자가 Mozilla 리눅스를 사용하는 것으로 확인



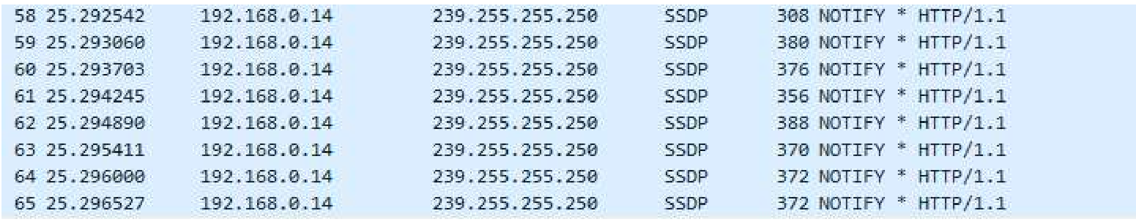
```
52 21.810624    fe80::2c0:26ff:fe2a… ff02::1:ff00:63    ICMPv6    86 Neighbor Solicitation for 2001:500:13::63 from 00:c0:26:2a:6e:b2
53 22.015562    JuniperNetwo 9a:f2:… Broadcast          ARP       60 Who has 192.168.0.47? Tell 192.168.0.1
```

패킷 51-52

: ICMPv6 프로토콜 기반의 Neighbor Solicitation(NS) 메시지, IPv6 네트워크 환경에서 연결된 이웃 장치를 찾기 위한 정상적인 동작.

패킷 53-56

: 로컬 네트워크 내에서 해당 IP 주소(192.168.0.47)의 MAC 주소를 알아내기 위해 브로드캐스트 요청을 전송



```
58 25.292542    192.168.0.14    239.255.255.250    SSDP    308 NOTIFY * HTTP/1.1
59 25.293060    192.168.0.14    239.255.255.250    SSDP    380 NOTIFY * HTTP/1.1
60 25.293703    192.168.0.14    239.255.255.250    SSDP    376 NOTIFY * HTTP/1.1
61 25.294245    192.168.0.14    239.255.255.250    SSDP    356 NOTIFY * HTTP/1.1
62 25.294890    192.168.0.14    239.255.255.250    SSDP    388 NOTIFY * HTTP/1.1
63 25.295411    192.168.0.14    239.255.255.250    SSDP    370 NOTIFY * HTTP/1.1
64 25.296000    192.168.0.14    239.255.255.250    SSDP    372 NOTIFY * HTTP/1.1
65 25.296527    192.168.0.14    239.255.255.250    SSDP    372 NOTIFY * HTTP/1.1
```

패킷 58-65

: SSDP NOTIFY 메시지가 연속적으로 전송됨

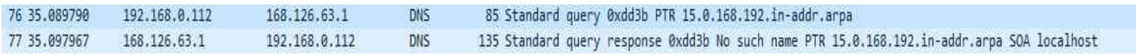
네트워크 장치들이 서로를 검색하고, 네트워크 서비스나 장치를 자동으로 발견하는 데 사용되는 프로토콜. SSDP는 주로 멀티캐스트 주소를 사용하여 다른 장치들에게 알림을 보내고 응답을 받음

패킷 66-79

: ARP 요청 계속 반복. 이전과 동일한 Who has 192.168.0.47? Tell 192.168.0.1 요청

패킷 73-75

: 브로드캐스트로 요청되었으며, 192.168.0.15에 대한 ARP 응답이 네트워크로 브로드캐스트. 응답에 따라 192.168.0.15의 MAC 주소(00:c0:26:2a:6e:b2)가 네트워크 상에 알려짐.

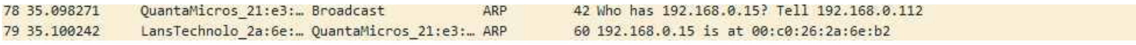


```
76 35.089790    192.168.0.112    168.126.63.1     DNS     85 Standard query 0xdd3b PTR 15.0.168.192.in-addr.arpa
77 35.097967    168.126.63.1     192.168.0.112    DNS    135 Standard query response 0xdd3b No such name PTR 15.0.168.192.in-addr.arpa SOA localhost
```

패킷 76-77

: DNS 요청이 15.0.168.192.in-addr.arpa 도메인에 대한 PTR (Reverse DNS Lookup). 주로 IP 주소를 도메인 이름으로 변환하기 위해 역방향 조회 수행

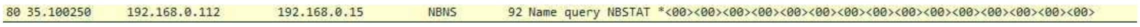
응답 내용: No such name PTR은 DNS 서버가 요청된 PTR 레코드에 대한 정보를 찾지 못했음을 의미



```
78 35.098271    QuantaMicros_21:e3:… Broadcast             ARP    42 Who has 192.168.0.15? Tell 192.168.0.112
79 35.100242    LansTechnolo_2a:6e:… QuantaMicros_21:e3:… ARP    60 192.168.0.15 is at 00:c0:26:2a:6e:b2
```

패킷 78~29

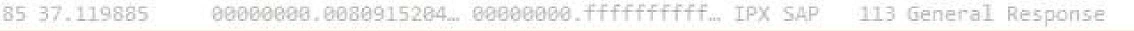
: 192.168.0.15의 MAC주소를 찾는 ARP프로토콜에 LansTechnolo_2a:6e:b2가 192.168.0.15라고 응답을 보냈음



```
80 35.100250    192.168.0.112    192.168.0.15    NBNS    92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
```

패킷 80

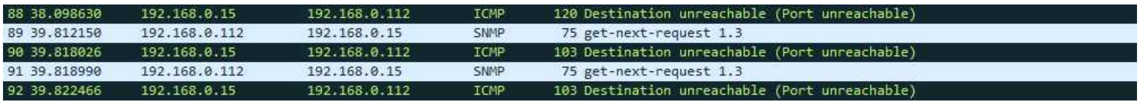
: NBNS = NetBIOS Name Service의 약자로 NetBIOS 이름을 사용하여 네트워크 상의 다른 장치들을 찾는데 사용되는 프로토콜, 네트워크 상에서 이름을 IP주소와 연결하는 역할을 한다. <00>으로 특정 이름을 나타내지 않았으므로 모든 네트워크 장치에서 응답을 받기 위한 질의



```
85 37.119885      00000000.0080915204… 00000000.ffffffffff… IPX SAP   113 General Response
```

패킷 85

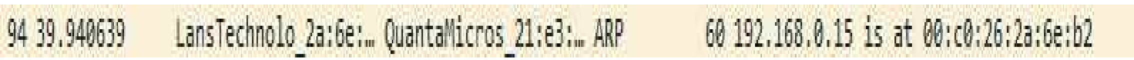
: 프로토콜: IPX SAP, 네트워크에서 서비스(예: 프린터, 파일 서버 등)를 광고하기 위해 사용되는 프로토콜



```
88 38.098630    192.168.0.15     192.168.0.112    ICMP    120 Destination unreachable (Port unreachable)
89 39.812150    192.168.0.112    192.168.0.15     SNMP     75 get-next-request 1.3
90 39.818026    192.168.0.15     192.168.0.112    ICMP    103 Destination unreachable (Port unreachable)
91 39.818990    192.168.0.112    192.168.0.15     SNMP     75 get-next-request 1.3
92 39.822466    192.168.0.15     192.168.0.112    ICMP    103 Destination unreachable (Port unreachable)
```

패킷 88-92

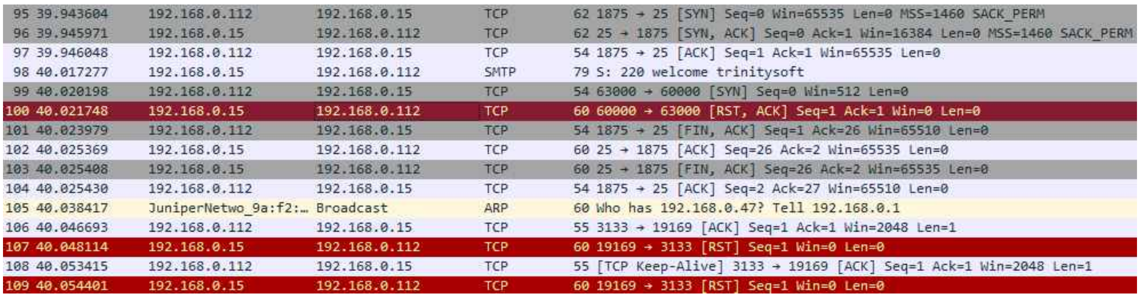
: 192.168.0.112는 SNMP Get-Next-Request 명령을 통해 192.168.0.15의 네트워크 정보를 요청했으나, 대상 포트가 닫혀있어 ICMP Destination Unreachable 응답을 수신



```
94 39.940639    LansTechnolo_2a:6e:… QuantaMicros_21:e3:… ARP    60 192.168.0.15 is at 00:c0:26:2a:6e:b2
```

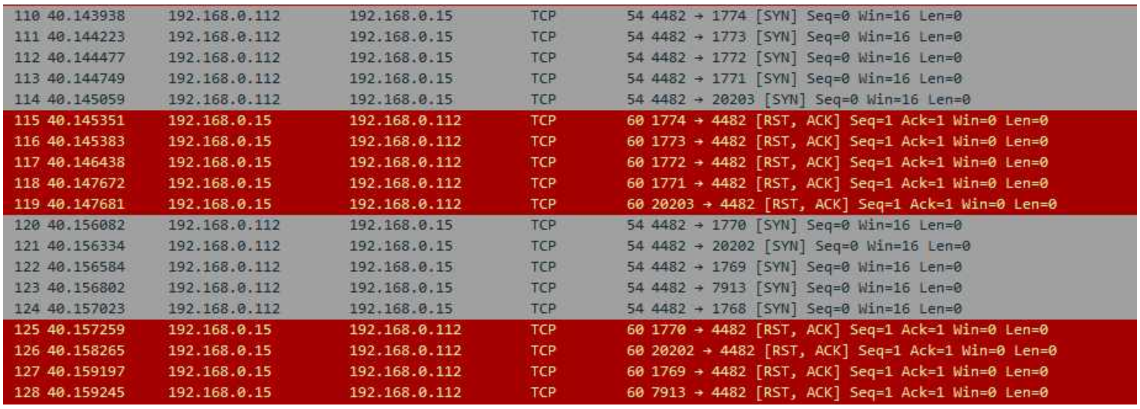
94

: 192.168.0.15의 mac 주소를 192.168.0.112에서 응답



```
 95 39.943604   192.168.0.112        192.168.0.15     TCP     62 1875 → 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
 96 39.945971   192.168.0.15         192.168.0.112    TCP     62 25 → 1875 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
 97 39.946048   192.168.0.112        192.168.0.15     TCP     54 1875 → 25 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 98 40.017277   192.168.0.15         192.168.0.112    SMTP    79 S: 220 welcome trinitysoft
 99 40.020198   192.168.0.112        192.168.0.15     TCP     54 63000 → 60000 [SYN] Seq=0 Win=512 Len=0
100 40.021748   192.168.0.15         192.168.0.112    TCP     60 60000 → 63000 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101 40.023979   192.168.0.112        192.168.0.15     TCP     54 1875 → 25 [FIN, ACK] Seq=1 Ack=26 Win=65510 Len=0
102 40.025369   192.168.0.15         192.168.0.112    TCP     60 25 → 1875 [ACK] Seq=26 Ack=2 Win=65535 Len=0
103 40.025408   192.168.0.15         192.168.0.112    TCP     60 25 → 1875 [FIN, ACK] Seq=26 Ack=2 Win=65535 Len=0
104 40.025430   192.168.0.112        192.168.0.15     TCP     54 1875 → 25 [ACK] Seq=2 Ack=27 Win=65510 Len=0
105 40.038417   JuniperNetwo_9a:f2:… Broadcast        ARP     60 Who has 192.168.0.47? Tell 192.168.0.1
106 40.046693   192.168.0.112        192.168.0.15     TCP     55 3133 → 19169 [ACK] Seq=1 Ack=1 Win=2048 Len=1
107 40.048114   192.168.0.15         192.168.0.112    TCP     60 19169 → 3133 [RST] Seq=1 Win=0 Len=0
108 40.053415   192.168.0.112        192.168.0.15     TCP     55 [TCP Keep-Alive] 3133 → 19169 [ACK] Seq=1 Ack=1 Win=2048 Len=1
109 40.054401   192.168.0.15         192.168.0.112    TCP     60 19169 → 3133 [RST] Seq=1 Win=0 Len=0
```

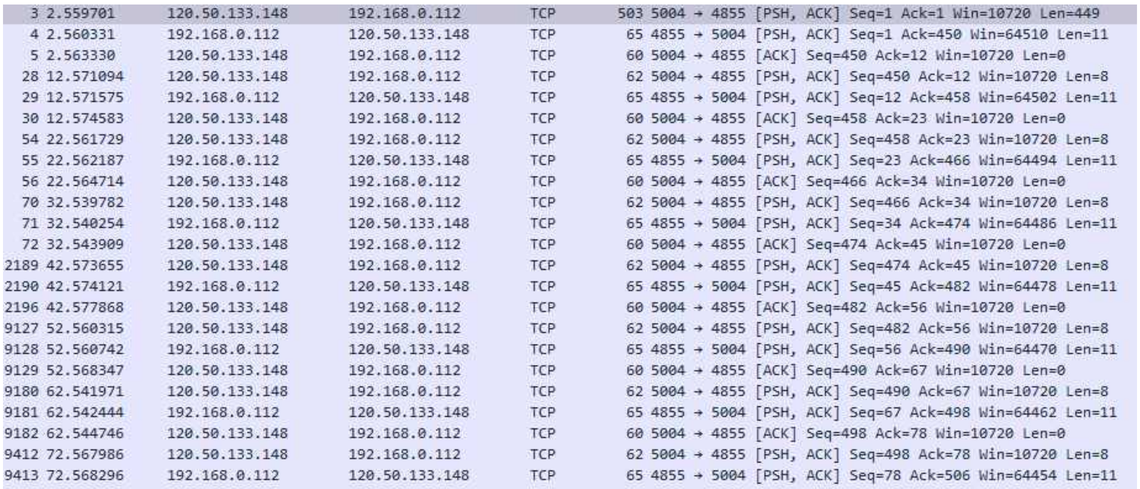
95번 패킷부터 이메일 시스템에 연결을 시도 하고 연결을 성공한 후 99번 패킷에서 새로운 포트로 연결을 시도 함. 중간자 공격이나 세션하이재킹의 공격 가능성이 있음 이후 3313포트에서 19169포트로 TCP 연결 유지에 대한 패킷을 보냄



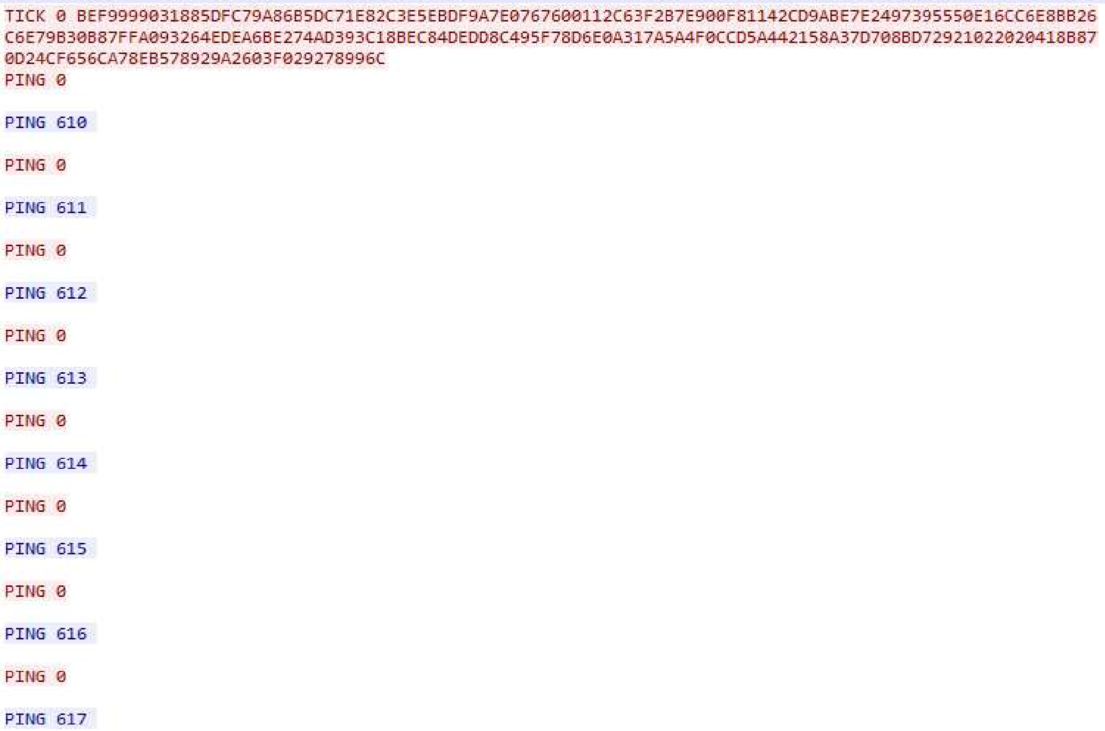
```
110 40.143938   192.168.0.112    192.168.0.15     TCP    54 4482 → 1774 [SYN] Seq=0 Win=16 Len=0
111 40.144223   192.168.0.112    192.168.0.15     TCP    54 4482 → 1773 [SYN] Seq=0 Win=16 Len=0
112 40.144477   192.168.0.112    192.168.0.15     TCP    54 4482 → 1772 [SYN] Seq=0 Win=16 Len=0
113 40.144749   192.168.0.112    192.168.0.15     TCP    54 4482 → 1771 [SYN] Seq=0 Win=16 Len=0
114 40.145059   192.168.0.112    192.168.0.15     TCP    54 4482 → 20203 [SYN] Seq=0 Win=16 Len=0
115 40.145351   192.168.0.15     192.168.0.112    TCP    60 1774 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116 40.145383   192.168.0.15     192.168.0.112    TCP    60 1773 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
117 40.146438   192.168.0.15     192.168.0.112    TCP    60 1772 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
118 40.147672   192.168.0.15     192.168.0.112    TCP    60 1771 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 40.147681   192.168.0.15     192.168.0.112    TCP    60 20203 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120 40.156082   192.168.0.112    192.168.0.15     TCP    54 4482 → 1770 [SYN] Seq=0 Win=16 Len=0
121 40.156334   192.168.0.112    192.168.0.15     TCP    54 4482 → 20202 [SYN] Seq=0 Win=16 Len=0
122 40.156584   192.168.0.112    192.168.0.15     TCP    54 4482 → 1769 [SYN] Seq=0 Win=16 Len=0
123 40.156802   192.168.0.112    192.168.0.15     TCP    54 4482 → 7913 [SYN] Seq=0 Win=16 Len=0
124 40.157023   192.168.0.112    192.168.0.15     TCP    54 4482 → 1768 [SYN] Seq=0 Win=16 Len=0
125 40.157259   192.168.0.15     192.168.0.112    TCP    60 1770 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
126 40.158265   192.168.0.15     192.168.0.112    TCP    60 20202 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
127 40.159197   192.168.0.15     192.168.0.112    TCP    60 1769 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128 40.159245   192.168.0.15     192.168.0.112    TCP    60 7913 → 4482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

이후 같은 IP에서 여러 포트로 SYN패킷을 보내는 것으로 보아 포트 스캐닝임을 의심

TCP 대화따라가기

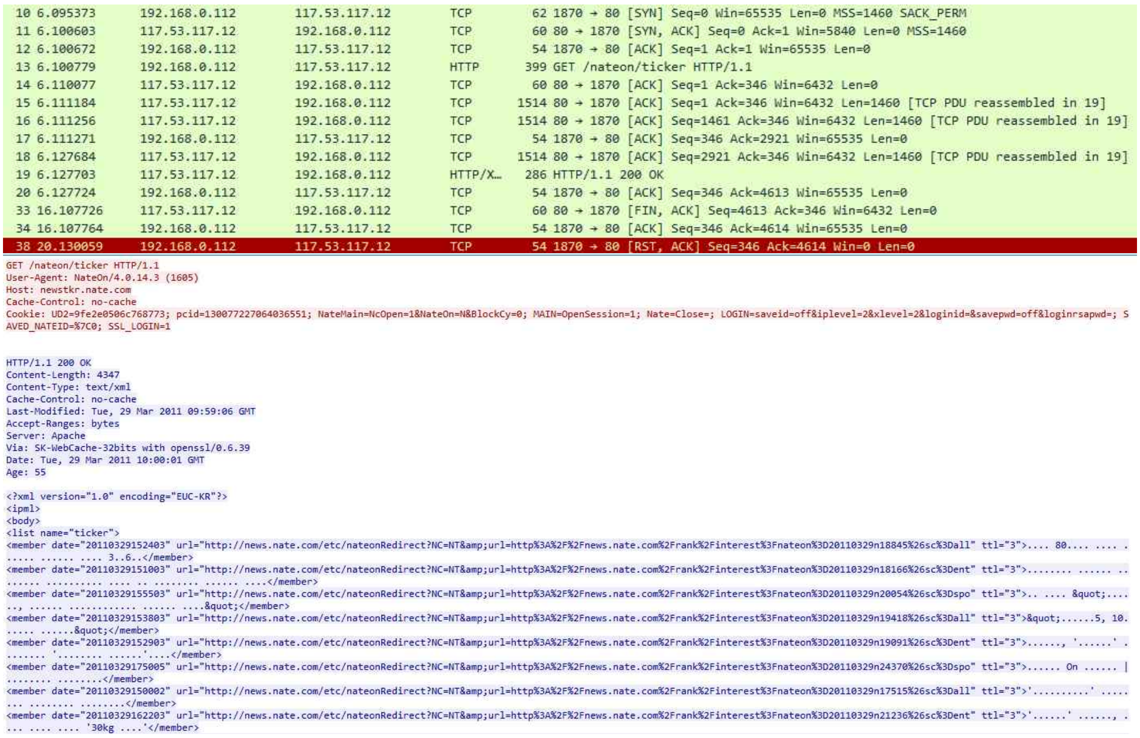


```
   3 2.559701     120.50.133.148     192.168.0.112      TCP        503 5004 → 4855 [PSH, ACK] Seq=1 Ack=1 Win=10720 Len=449
   4 2.560331     192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=1 Ack=450 Win=64510 Len=11
   5 2.563330     120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=450 Ack=12 Win=10720 Len=0
  28 12.571094    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=450 Ack=12 Win=10720 Len=8
  29 12.571575    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=12 Ack=458 Win=64502 Len=11
  30 12.574583    120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=458 Ack=23 Win=10720 Len=0
  54 22.561729    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=458 Ack=23 Win=10720 Len=8
  55 22.562187    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=23 Ack=466 Win=64494 Len=11
  56 22.564714    120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=466 Ack=34 Win=10720 Len=0
  70 32.539782    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=466 Ack=34 Win=10720 Len=8
  71 32.540254    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=34 Ack=474 Win=64486 Len=11
  72 32.543909    120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=474 Ack=45 Win=10720 Len=0
2189 42.573655    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=474 Ack=45 Win=10720 Len=8
2190 42.574121    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=45 Ack=482 Win=64478 Len=11
2196 42.577868    120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=482 Ack=56 Win=10720 Len=0
9127 52.560315    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=482 Ack=56 Win=10720 Len=8
9128 52.560742    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=56 Ack=490 Win=64470 Len=11
9129 52.568347    120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=490 Ack=67 Win=10720 Len=0
9180 62.541971    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=490 Ack=67 Win=10720 Len=8
9181 62.542444    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=67 Ack=498 Win=64462 Len=11
9182 62.544746    120.50.133.148     192.168.0.112      TCP         60 5004 → 4855 [ACK] Seq=498 Ack=78 Win=10720 Len=0
9412 72.567986    120.50.133.148     192.168.0.112      TCP         62 5004 → 4855 [PSH, ACK] Seq=498 Ack=78 Win=10720 Len=8
9413 72.568296    192.168.0.112      120.50.133.148     TCP         65 4855 → 5004 [PSH, ACK] Seq=78 Ack=506 Win=64454 Len=11
```



```
TICK 0 BEF9999031885DFC79A86B5DC71E82C3E5EBDF9A7E0767600112C63F2B7E900F81142CD9ABE7E2497395550E16CC6E8BB26
C6E79B30B87FFA093264EDEA6BE274AD393C18BEC84DEDD8C495F78D6E0A317A5A4F0CCD5A442158A37D708BD72921022020418B87
0D24CF656CA78EB578929A2603F029278996C
PING 0

PING 610

PING 0

PING 611

PING 0

PING 612

PING 0

PING 613

PING 0

PING 614

PING 0

PING 615

PING 0

PING 616

PING 0

PING 617
```

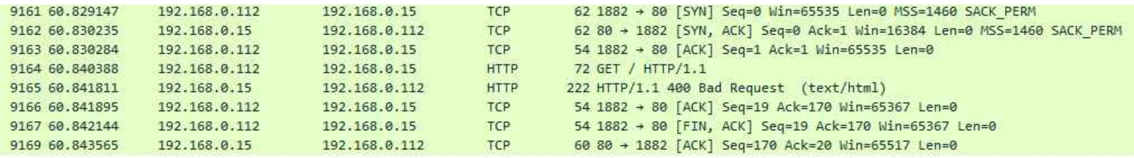
지속적으로 PING명령어를 실행하는 것으로 보임



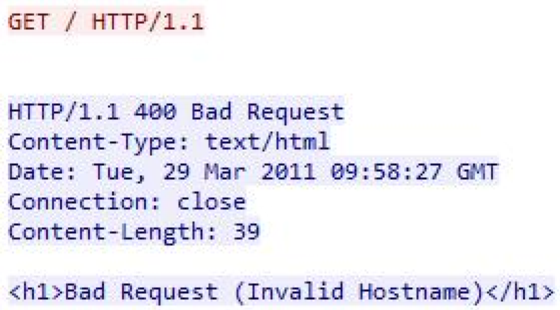
```
 10 6.095373    192.168.0.112     117.53.117.12     TCP       62 1870 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
 11 6.100603    117.53.117.12     192.168.0.112     TCP       60 80 → 1870 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 12 6.100672    192.168.0.112     117.53.117.12     TCP       54 1870 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 13 6.100779    192.168.0.112     117.53.117.12     HTTP     399 GET /nateon/ticker HTTP/1.1
 14 6.110077    117.53.117.12     192.168.0.112     TCP       60 80 → 1870 [ACK] Seq=1 Ack=346 Win=6432 Len=0
 15 6.111184    117.53.117.12     192.168.0.112     TCP     1514 80 → 1870 [ACK] Seq=1 Ack=346 Win=6432 Len=1460 [TCP PDU reassembled in 19]
 16 6.111256    117.53.117.12     192.168.0.112     TCP     1514 80 → 1870 [ACK] Seq=1461 Ack=346 Win=6432 Len=1460 [TCP PDU reassembled in 19]
 17 6.111271    192.168.0.112     117.53.117.12     TCP       54 1870 → 80 [ACK] Seq=346 Ack=2921 Win=65535 Len=0
 18 6.127684    117.53.117.12     192.168.0.112     TCP     1514 80 → 1870 [ACK] Seq=2921 Ack=346 Win=6432 Len=1460 [TCP PDU reassembled in 19]
 19 6.127703    117.53.117.12     192.168.0.112     HTTP/X…  286 HTTP/1.1 200 OK
 20 6.127724    192.168.0.112     117.53.117.12     TCP       54 1870 → 80 [ACK] Seq=346 Ack=4613 Win=65535 Len=0
 33 16.107726   117.53.117.12     192.168.0.112     TCP       60 80 → 1870 [FIN, ACK] Seq=4613 Ack=346 Win=6432 Len=0
 34 16.107764   192.168.0.112     117.53.117.12     TCP       54 1870 → 80 [ACK] Seq=346 Ack=4614 Win=65535 Len=0
 38 20.130059   192.168.0.112     117.53.117.12     TCP       54 1870 → 80 [RST, ACK] Seq=346 Ack=4614 Win=0 Len=0
```

```
GET /nateon/ticker HTTP/1.1
User-Agent: NateOn/4.0.14.3 (1605)
Host: newstkr.nate.com
Cache-Control: no-cache
Cookie: UD2=9fe2e0506c768773; pcid=130077227064036551; NateMain=NcOpen=1&NateOn=N&BlockCy=0; MAIN=OpenSession=1; Nate=Close=; LOGIN=saveid=off&iplevel=2&xlevel=2&loginid=&savepwd=off&loginrsapwd=; S
AVED_NATEID=%7C0; SSL_LOGIN=1


HTTP/1.1 200 OK
Content-Length: 4347
Content-Type: text/xml
Cache-Control: no-cache
Last-Modified: Tue, 29 Mar 2011 09:59:06 GMT
Accept-Ranges: bytes
Server: Apache
Via: SK-WebCache-32bits with openssl/0.6.39
Date: Tue, 29 Mar 2011 10:00:01 GMT
Age: 55

<?xml version="1.0" encoding="EUC-KR"?>
<ipml>
<body>
<list name="ticker">
<member date="20110329152403" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n18845%26sc%3Dall" ttl="3">.... 80.... ..... .
..... ...... .... 3..6..</member>
<member date="20110329151003" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n18166%26sc%3Dent" ttl="3">........ ...... ..
...... .......... .... .. ........ ...... ....</member>
<member date="20110329155503" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n20054%26sc%3Dspo" ttl="3">.. .... &quot;....
.., ...... ............ ...... ....&quot;</member>
<member date="20110329153803" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n19418%26sc%3Dall" ttl="3">&quot;......5, 10.
..... ......&quot;</member>
<member date="20110329152903" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n19091%26sc%3Dent" ttl="3">......, '......' .
....... '........ ......'....</member>
<member date="20110329175005" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n24370%26sc%3Dspo" ttl="3">...... On ...... |
........ ........</member>
<member date="20110329150002" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n17515%26sc%3Dall" ttl="3">'..........' .....
... ........ ........</member>
<member date="20110329162203" url="http://news.nate.com/etc/nateonRedirect?NC=NT&amp;url=http%3A%2F%2Fnews.nate.com%2Frank%2Finterest%3Fnateon%3D20110329n21236%26sc%3Dent" ttl="3">'......' ......, .
... .... .... '30kg ....'</member>
```

nate의 news에 접속하여 받은 html코드

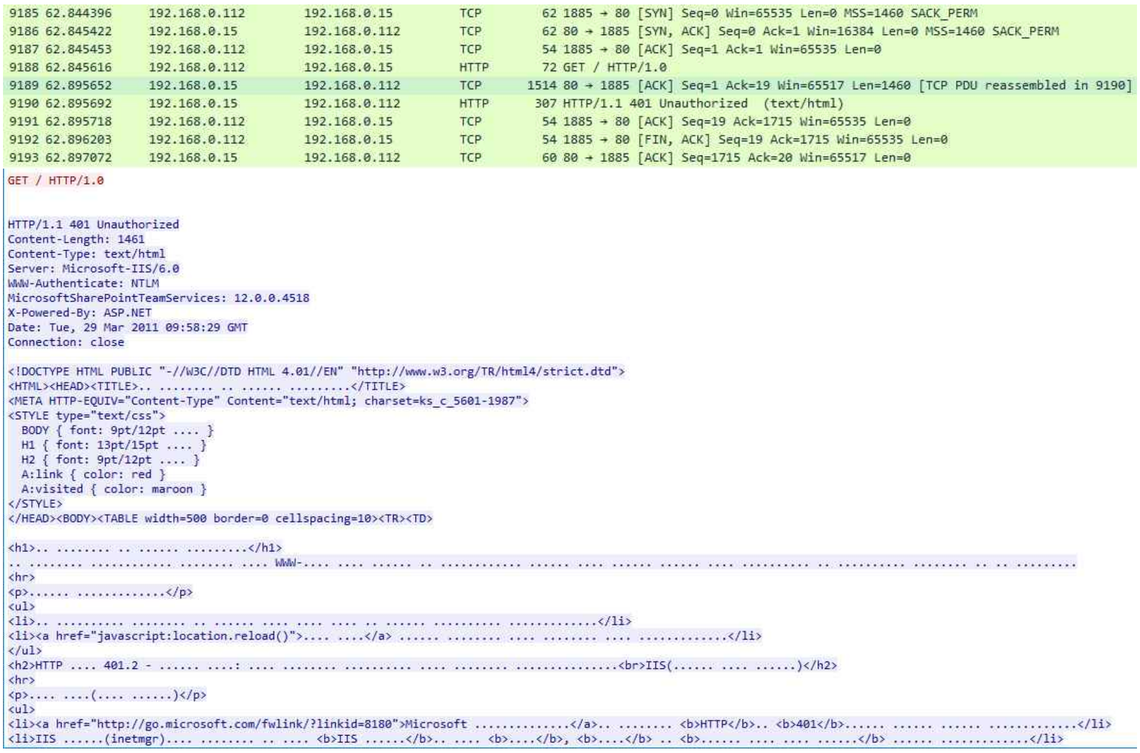


```
9161 60.829147    192.168.0.112     192.168.0.15      TCP        62 1882 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9162 60.830235    192.168.0.15      192.168.0.112     TCP        62 80 → 1882 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
9163 60.830284    192.168.0.112     192.168.0.15      TCP        54 1882 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9164 60.840388    192.168.0.112     192.168.0.15      HTTP       72 GET / HTTP/1.1
9165 60.841811    192.168.0.15      192.168.0.112     HTTP      222 HTTP/1.1 400 Bad Request  (text/html)
9166 60.841895    192.168.0.112     192.168.0.15      TCP        54 1882 → 80 [ACK] Seq=19 Ack=170 Win=65367 Len=0
9167 60.842144    192.168.0.112     192.168.0.15      TCP        54 1882 → 80 [FIN, ACK] Seq=19 Ack=170 Win=65367 Len=0
9169 60.843565    192.168.0.15      192.168.0.112     TCP        60 80 → 1882 [ACK] Seq=170 Ack=20 Win=65517 Len=0
```



```
GET / HTTP/1.1


HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Tue, 29 Mar 2011 09:58:27 GMT
Connection: close
Content-Length: 39

<h1>Bad Request (Invalid Hostname)</h1>
```

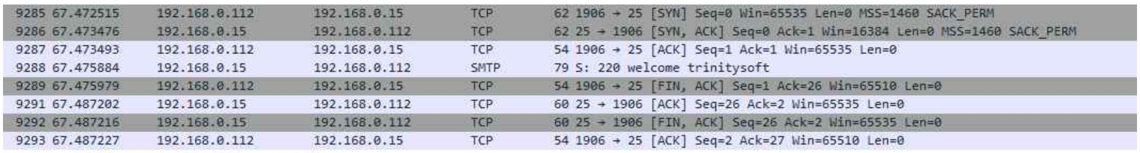
클라이언트가 보낸 요청에 오류가 있는 HTTP 400 Bad Request패킷



```
9185 62.844396   192.168.0.112   192.168.0.15    TCP     62 1885 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9186 62.845422   192.168.0.15    192.168.0.112   TCP     62 80 → 1885 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
9187 62.845453   192.168.0.112   192.168.0.15    TCP     54 1885 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9188 62.845616   192.168.0.112   192.168.0.15    HTTP    72 GET / HTTP/1.0
9189 62.895652   192.168.0.15    192.168.0.112   TCP   1514 80 → 1885 [ACK] Seq=1 Ack=19 Win=65517 Len=1460 [TCP PDU reassembled in 9190]
9190 62.895692   192.168.0.15    192.168.0.112   HTTP   307 HTTP/1.1 401 Unauthorized  (text/html)
9191 62.895718   192.168.0.112   192.168.0.15    TCP     54 1885 → 80 [ACK] Seq=19 Ack=1715 Win=65535 Len=0
9192 62.896203   192.168.0.112   192.168.0.15    TCP     54 1885 → 80 [FIN, ACK] Seq=19 Ack=1715 Win=65535 Len=0
9193 62.897072   192.168.0.15    192.168.0.112   TCP     60 80 → 1885 [ACK] Seq=1715 Ack=20 Win=65517 Len=0
```

```
GET / HTTP/1.0


HTTP/1.1 401 Unauthorized
Content-Length: 1461
Content-Type: text/html
Server: Microsoft-IIS/6.0
WWW-Authenticate: NTLM
MicrosoftSharePointTeamServices: 12.0.0.4518
X-Powered-By: ASP.NET
Date: Tue, 29 Mar 2011 09:58:29 GMT
Connection: close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>.. ........ .. ...... .........</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=ks_c_5601-1987">
<STYLE type="text/css">
  BODY { font: 9pt/12pt .... }
  H1 { font: 13pt/15pt .... }
  H2 { font: 9pt/12pt .... }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>

<h1>.. ........ .. ...... .........</h1>
.. ........ ............ ........ .... WWW-.... .... ...... .. ............ ...... .... ...... ...... .... .......... .. .......... ........ .. .. .........
<hr>
<p>...... .............</p>
<ul>
<li>.. .......... ........ .. ...... .... .... .... .. ...... .......... .............</li>
<li><a href="javascript:location.reload()">.... ....</a> ...... ........ .... ........ .... .............</li>
</ul>
<h2>HTTP .... 401.2 - ...... ....: .... ........ .......... .... ........ ...............<br>IIS(...... .... ......)</h2>
<hr>
<p>.... ....(.... ......)</p>
<ul>
<li><a href="http://go.microsoft.com/fwlink/?linkid=8180">Microsoft .............</a>.. ........ <b>HTTP</b>.. <b>401</b>...... ...... ...... ............</li>
<li>IIS ......(inetmgr).... ........ .. .... <b>IIS ......</b>.. .... <b>....</b>, <b>....</b> .. <b>...... .... .... ......</b> ...... .............</li>
```

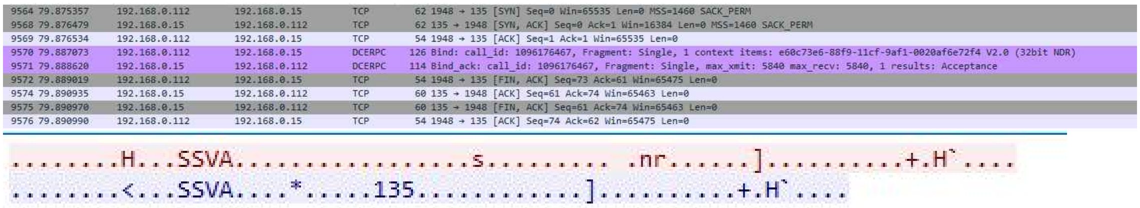
401 Unauthorized : 클라이언트가 요청한 리소스에 접근할 권한이 없다는 것을 나타내는 HTTP 상태 코드



```
9285 67.472515   192.168.0.112   192.168.0.15    TCP    62 1906 → 25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9286 67.473476   192.168.0.15    192.168.0.112   TCP    62 25 → 1906 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
9287 67.473493   192.168.0.112   192.168.0.15    TCP    54 1906 → 25 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9288 67.475884   192.168.0.15    192.168.0.112   SMTP   79 S: 220 welcome trinitysoft
9289 67.475979   192.168.0.112   192.168.0.15    TCP    54 1906 → 25 [FIN, ACK] Seq=1 Ack=26 Win=65510 Len=0
9291 67.487202   192.168.0.15    192.168.0.112   TCP    60 25 → 1906 [ACK] Seq=26 Ack=2 Win=65535 Len=0
9292 67.487216   192.168.0.15    192.168.0.112   TCP    60 25 → 1906 [FIN, ACK] Seq=26 Ack=2 Win=65535 Len=0
9293 67.487227   192.168.0.112   192.168.0.15    TCP    54 1906 → 25 [ACK] Seq=2 Ack=27 Win=65510 Len=0
```

```
220 welcome trinitysoft
```

SMTP 메시지 서비스에 연결



```
9564 79.875357   192.168.0.112   192.168.0.15    TCP      62 1948 → 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9568 79.876479   192.168.0.15    192.168.0.112   TCP      62 135 → 1948 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
9569 79.876534   192.168.0.112   192.168.0.15    TCP      54 1948 → 135 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9570 79.887073   192.168.0.112   192.168.0.15    DCERPC  126 Bind: call_id: 1096176467, Fragment: Single, 1 context items: e60c73e6-88f9-11cf-9af1-0020af6e72f4 V2.0 (32bit NDR)
9571 79.888620   192.168.0.15    192.168.0.112   DCERPC  114 Bind_ack: call_id: 1096176467, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
9572 79.889019   192.168.0.112   192.168.0.15    TCP      54 1948 → 135 [FIN, ACK] Seq=73 Ack=61 Win=65475 Len=0
9574 79.890935   192.168.0.15    192.168.0.112   TCP      60 135 → 1948 [ACK] Seq=61 Ack=74 Win=65463 Len=0
9575 79.890970   192.168.0.15    192.168.0.112   TCP      60 135 → 1948 [FIN, ACK] Seq=61 Ack=74 Win=65463 Len=0
9576 79.890990   192.168.0.112   192.168.0.15    TCP      54 1948 → 135 [ACK] Seq=74 Ack=62 Win=65475 Len=0
```

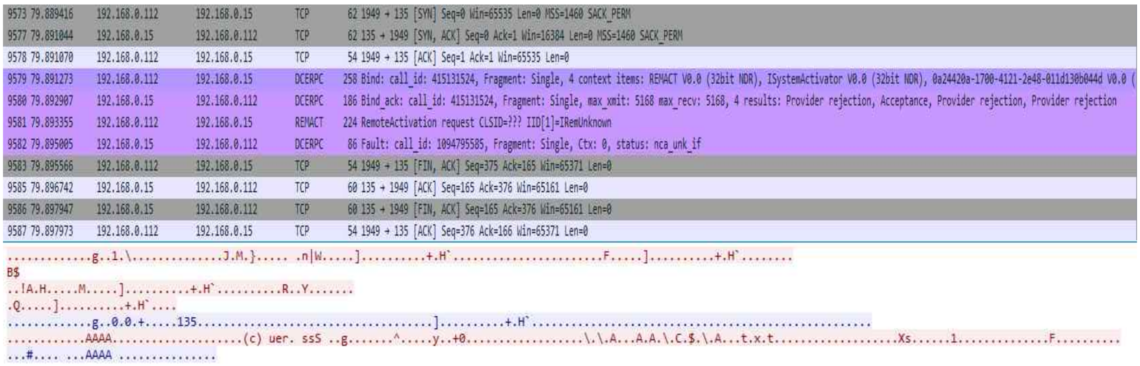
```
........H...SSVA..................s.........  .nr......]..........+.H`....
........<...SSVA....*.....135............]..........+.H`....
```

DCERPC (Distributed Computing Environment / Remote Procedure Call)

원격 프로시저 호출 (RPC)의 한 형태로, 분산 환경에서 다른 시스템의 프로시저(함수나 메소드)를 호출할 수 있게 해주는 프로토콜

DCE (Distributed Computing Environment)라는 프레임워크의 일부로, 다양한 시스템 간에 분산 애플리케이션을 개발할 수 있게 지원하는 기술

TCP 연결을 설정하고, DCERPC 프로토콜을 사용하여 Bind 요청과 응답을 교환하는 과정. 그 후, 연결을 종료하는 FIN, ACK 패킷이 교환



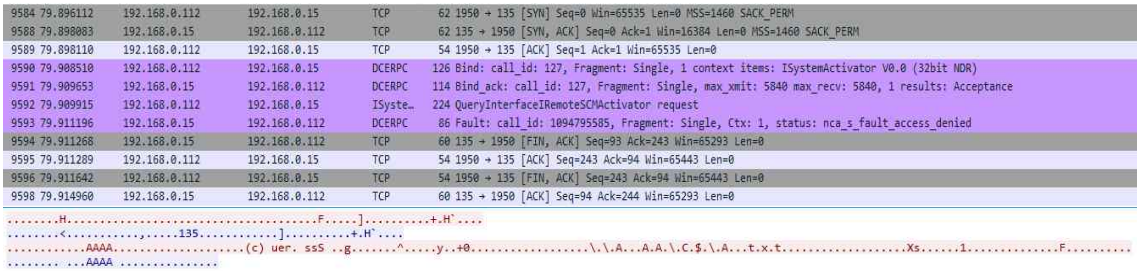
```
9573 79.889416   192.168.0.112   192.168.0.15    TCP      62 1949 → 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9577 79.891044   192.168.0.15    192.168.0.112   TCP      62 135 → 1949 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
9578 79.891070   192.168.0.112   192.168.0.15    TCP      54 1949 → 135 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9579 79.891273   192.168.0.112   192.168.0.15    DCERPC  258 Bind: call_id: 415131524, Fragment: Single, 4 context items: REMACT V0.0 (32bit NDR), ISystemActivator V0.0 (32bit NDR), 0a24420a-1700-4121-2e48-011d130b044d V0.0 (
9580 79.892907   192.168.0.15    192.168.0.112   DCERPC  186 Bind_ack: call_id: 415131524, Fragment: Single, max_xmit: 5168 max_recv: 5168, 4 results: Provider rejection, Acceptance, Provider rejection, Provider rejection
9581 79.893355   192.168.0.112   192.168.0.15    REMACT  224 RemoteActivation request CLSID=??? IID[1]=IRemUnknown
9582 79.895005   192.168.0.15    192.168.0.112   DCERPC   86 Fault: call_id: 1094795585, Fragment: Single, Ctx: 0, status: nca_unk_if
9583 79.895566   192.168.0.112   192.168.0.15    TCP      54 1949 → 135 [FIN, ACK] Seq=375 Ack=165 Win=65371 Len=0
9585 79.896742   192.168.0.15    192.168.0.112   TCP      60 135 → 1949 [ACK] Seq=165 Ack=376 Win=65161 Len=0
9586 79.897947   192.168.0.15    192.168.0.112   TCP      60 135 → 1949 [FIN, ACK] Seq=165 Ack=376 Win=65161 Len=0
9587 79.897973   192.168.0.112   192.168.0.15    TCP      54 1949 → 135 [ACK] Seq=376 Ack=166 Win=65371 Len=0
```

```
.............g..1.\..............J.M.}..... .n|W.....]..........+.H`......................F.....]..........+.H`........
B$
..!A.H.....M.....]..........+.H`..........R..Y.......
.Q.....]..........+.H`....
.............g..0.0.+.....135..................................]..........+.H`..................................................
............AAAA...................(c) uer. ssS ..g.......^.....y..+0.................\.\.A...A.A.\.C.$.\.A...t.x.t...................Xs......1.............F.........
...#.... ...AAAA ...............
```

DCERPC 프로토콜을 사용한 원격 프로시저 호출 요청과 응답

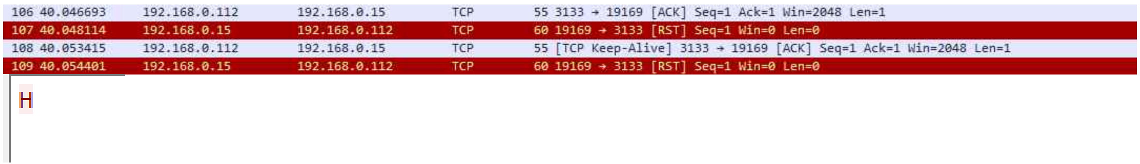
Bind 요청 후 Provider rejection이 발생하는 등, 요청이 거부되고 연결이 종료

Fault 응답에서 nca_unk_if오류가 발생 = 알 수 없는 인터페이스 오류로 요청이 처리 되지 않음을 의미



```
9584 79.896112   192.168.0.112   192.168.0.15    TCP       62 1950 → 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9588 79.898083   192.168.0.15    192.168.0.112   TCP       62 135 → 1950 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM
9589 79.898110   192.168.0.112   192.168.0.15    TCP       54 1950 → 135 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9590 79.908510   192.168.0.112   192.168.0.15    DCERPC   126 Bind: call_id: 127, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR)
9591 79.909653   192.168.0.15    192.168.0.112   DCERPC   114 Bind_ack: call_id: 127, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
9592 79.909915   192.168.0.112   192.168.0.15    ISyste…  224 QueryInterfaceIRemoteSCMActivator request
9593 79.911196   192.168.0.15    192.168.0.112   DCERPC    86 Fault: call_id: 1094795585, Fragment: Single, Ctx: 1, status: nca_s_fault_access_denied
9594 79.911268   192.168.0.15    192.168.0.112   TCP       60 135 → 1950 [FIN, ACK] Seq=93 Ack=243 Win=65293 Len=0
9595 79.911289   192.168.0.112   192.168.0.15    TCP       54 1950 → 135 [ACK] Seq=243 Ack=94 Win=65443 Len=0
9596 79.911642   192.168.0.112   192.168.0.15    TCP       54 1950 → 135 [FIN, ACK] Seq=243 Ack=94 Win=65443 Len=0
9598 79.914960   192.168.0.15    192.168.0.112   TCP       60 135 → 1950 [ACK] Seq=94 Ack=244 Win=65293 Len=0
```

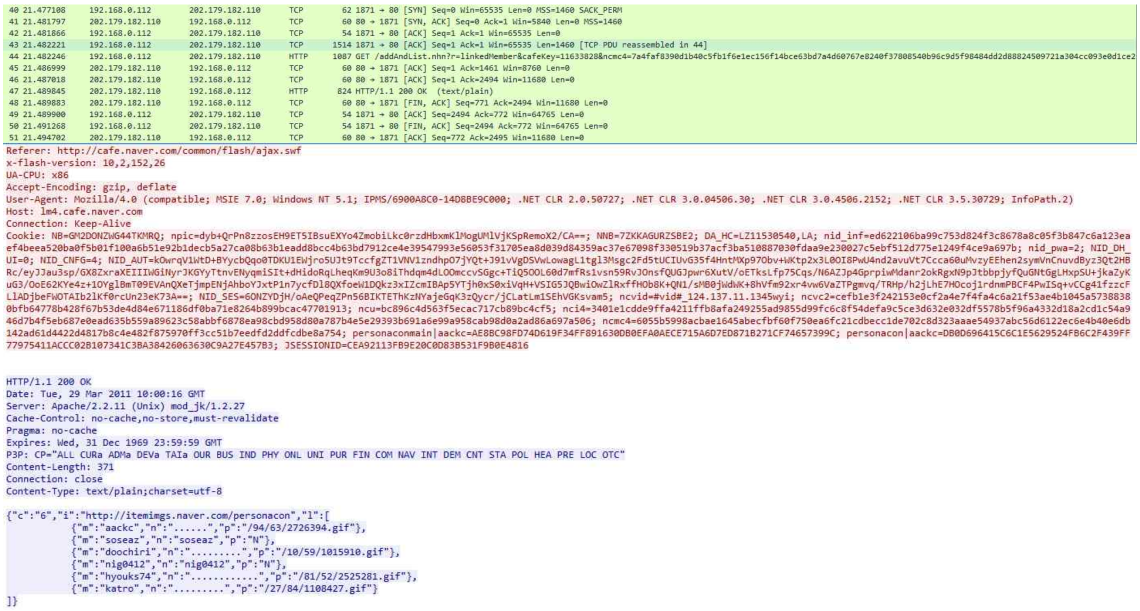
```
........H.....................................F.....]..........+.H`....
........<...........,.....135............]..........+.H`....
............AAAA...................(c) uer. ssS ..g.......^.....y..+0.................\.\.A...A.A.\.C.$.\.A...t.x.t...................Xs......1.............F.........
........ ...AAAA ...............
```



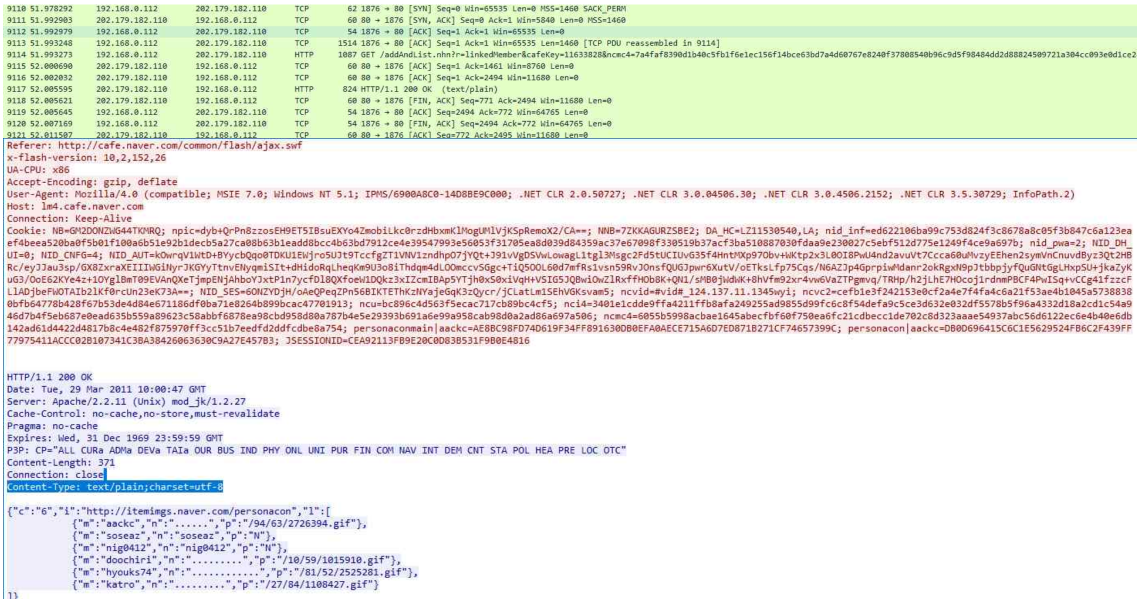
```
106 40.046693    192.168.0.112    192.168.0.15     TCP      55 3133 → 19169 [ACK] Seq=1 Ack=1 Win=2048 Len=1
107 40.048114    192.168.0.15     192.168.0.112    TCP      60 19169 → 3133 [RST] Seq=1 Win=0 Len=0
108 40.053415    192.168.0.112    192.168.0.15     TCP      55 [TCP Keep-Alive] 3133 → 19169 [ACK] Seq=1 Ack=1 Win=2048 Len=1
109 40.054401    192.168.0.15     192.168.0.112    TCP      60 19169 → 3133 [RST] Seq=1 Win=0 Len=0
```

```
H
```

연결을 유지 하려고 하지만 연결을 서버에서 끊음



```
40 21.477108   192.168.0.112     202.179.182.110   TCP     62 1871 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
41 21.481797   202.179.182.110   192.168.0.112     TCP     60 80 → 1871 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
42 21.481866   192.168.0.112     202.179.182.110   TCP     54 1871 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
43 21.482221   192.168.0.112     202.179.182.110   TCP   1514 1871 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=1460 [TCP PDU reassembled in 44]
44 21.482246   192.168.0.112     202.179.182.110   HTTP  1087 GET /addAndList.nhn?r=linkedMember&cafeKey=11633828&ncmc4=7a4faf8390d1b40c5fb1f6e1ec156f14bce63bd7a4d60767e8240f37808540b96c9d5f98484dd2d88824509721a304cc093e0d1ce2
45 21.486999   202.179.182.110   192.168.0.112     TCP     60 80 → 1871 [ACK] Seq=1 Ack=1461 Win=8760 Len=0
46 21.487018   202.179.182.110   192.168.0.112     TCP     60 80 → 1871 [ACK] Seq=1 Ack=2494 Win=11680 Len=0
47 21.489845   202.179.182.110   192.168.0.112     HTTP   824 HTTP/1.1 200 OK  (text/plain)
48 21.489883   202.179.182.110   192.168.0.112     TCP     60 80 → 1871 [FIN, ACK] Seq=771 Ack=2494 Win=11680 Len=0
49 21.489900   192.168.0.112     202.179.182.110   TCP     54 1871 → 80 [ACK] Seq=2494 Ack=772 Win=64765 Len=0
50 21.491268   192.168.0.112     202.179.182.110   TCP     54 1871 → 80 [FIN, ACK] Seq=2494 Ack=772 Win=64765 Len=0
51 21.494702   202.179.182.110   192.168.0.112     TCP     60 80 → 1871 [ACK] Seq=772 Ack=2495 Win=11680 Len=0
Referer: http://cafe.naver.com/common/flash/ajax.swf
x-flash-version: 10,2,152,26
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/6900A8C0-14D8BE9C000; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: lm4.cafe.naver.com
Connection: Keep-Alive
Cookie: NB=GM2DONZWG44TKMRQ; npic=dyb+QrPn8zzosEH9ET5IBsuEXYo4ZmobiLkc0rzdHbxmKlMogUMlVjKSpRemoX2/CA==; NNB=7ZKKAGURZSBE2; DA_HC=LZ11530540,LA; nid_inf=ed622106ba99c753d824f3c8678a8c05f3b847c6a123ea
ef4beea520ba0f5b01f100a6b51e92b1decb5a27ca08b63b1eadd8bcc4b63bd7912ce4e39547993e56053f31705ea8d039d84359ac37e67098f330519b37acf3ba510887030fdaa9e230027c5ebf512d775e1249f4ce9a697b; nid_pwa=2; NID_DH_
UI=0; NID_CNFG=4; NID_AUT=kOwrqV1WtD+BYycbQqo0TDKU1EWjro5UJt9TccfgZT1VNV1zndhpO7jYQt+J91vVgDSVwLowagL1tgl3Msgc2Fd5tUCIUvG35f4HntMXp97Obv+WKtp2x3L0OI8PwU4nd2avuVt7Ccca60uMvzyEEhen2symVnCnuvdByz3Qt2HB
Rc/eyJJau3sp/GX8ZxraXEIIIWGiNyrJKGYyTtnvENyqmiSIt+dHidoRqLheqKm9U3o8iThdqm4dLOOmccvSGgc+TiQ5OOL60d7mfRs1vsn59RvJOnsfQUGJpwr6XutV/oETksLfp75Cqs/N6AZJp4GprpiwMdanr2okRgxN9pJtbbpjyfQuGNtGgLHxpSU+jkaZyK
uG3/OoE62KYe4z+1OYglBmT09EVAnQXeTjmpENjAhboYJxtP1n7ycfDl8QXfoeW1DQkz3xIZcmIBAp5YTjh0xS0xiVqH+VSIG5JQBwiOwZlRxffHOb8K+QN1/sMB0jWdWK+8hVfm92xr4vw6VaZTPgmvq/TRHp/h2jLhE7HOcoj1rdnmPBCF4PwISq+vCCg41fzzcF
LlADjbeFWOTAIb2lKf0rcUn23eK73A==; NID_SES=6ONZYDjH/oAeQPeqZPn56BIKTEThKzNYajeGqK3zQycr/jCLatLm1SEhVGKsvam5; ncvid=#vid#_124.137.11.1345wyi; ncvc2=cefb1e3f242153e0cf2a4e7f4fa4c6a21f53ae4b1045a5738838
0bfb64778b428f67b53de4d84e671186df0ba71e8264b899bcac47701913; ncu=bc896c4d563f5ecac717cb89bc4cf5; nci4=3401e1cdde9ffa4211ffb8afa249255ad9855d99fc6c8f54defa9c5ce3d632e032df5578b5f96a4332d18a2cd1c54a9
46d7b4f5eb687e0ead635b559a89623c58abbf6878ea98cbd958d80a787b4e5e29393b691a6e99a958cab98d0a2ad86a697a506; ncmc4=6055b5998acbae1645abecfbf60f750ea6fc21cdbecc1de702c8d323aaae54937abc56d6122ec6e4b40e6db
142ad61d4422d4817b8c4e482f875970ff3cc51b7eedfd2ddfcdbe8a754; personaconmain|aackc=AE8BC98FD74D619F34FF891630DB0EFA0AECE715A6D7ED871B271CF74657399C; personacon|aackc=DB0D696415C6C1E5629524FB6C2F439FF
77975411ACCC02B107341C3BA38426063630C9A27E457B3; JSESSIONID=CEA92113FB9E20C0D83B531F9B0E4816


HTTP/1.1 200 OK
Date: Tue, 29 Mar 2011 10:00:16 GMT
Server: Apache/2.2.11 (Unix) mod_jk/1.2.27
Cache-Control: no-cache,no-store,must-revalidate
Pragma: no-cache
Expires: Wed, 31 Dec 1969 23:59:59 GMT
P3P: CP="ALL CURa ADMa DEVa TAIa OUR BUS IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC OTC"
Content-Length: 371
Connection: close
Content-Type: text/plain;charset=utf-8

{"c":"6","i":"http://itemimgs.naver.com/personacon","l":[
          {"m":"aackc","n":"......","p":"/94/63/2726394.gif"},
          {"m":"soseaz","n":"soseaz","p":"N"},
          {"m":"doochiri","n":".........","p":"/10/59/1015910.gif"},
          {"m":"nig0412","n":"nig0412","p":"N"},
          {"m":"hyouks74","n":"............","p":"/81/52/2525281.gif"},
          {"m":"katro","n":".........","p":"/27/84/1108427.gif"}
]}
```



```
9110 51.978292   192.168.0.112     202.179.182.110   TCP     62 1876 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
9111 51.992903   202.179.182.110   192.168.0.112     TCP     60 80 → 1876 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9112 51.992979   192.168.0.112     202.179.182.110   TCP     54 1876 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
9113 51.993248   192.168.0.112     202.179.182.110   TCP   1514 1876 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=1460 [TCP PDU reassembled in 9114]
9114 51.993273   192.168.0.112     202.179.182.110   HTTP  1087 GET /addAndList.nhn?r=linkedMember&cafeKey=11633828&ncmc4=7a4faf8390d1b40c5fb1f6e1ec156f14bce63bd7a4d60767e8240f37808540b96c9d5f98484dd2d88824509721a304cc093e0d1ce2
9115 52.000690   202.179.182.110   192.168.0.112     TCP     60 80 → 1876 [ACK] Seq=1 Ack=1461 Win=8760 Len=0
9116 52.002032   202.179.182.110   192.168.0.112     TCP     60 80 → 1876 [ACK] Seq=1 Ack=2494 Win=11680 Len=0
9117 52.005595   202.179.182.110   192.168.0.112     HTTP   824 HTTP/1.1 200 OK  (text/plain)
9118 52.005621   202.179.182.110   192.168.0.112     TCP     60 80 → 1876 [FIN, ACK] Seq=771 Ack=2494 Win=11680 Len=0
9119 52.005645   192.168.0.112     202.179.182.110   TCP     54 1876 → 80 [ACK] Seq=2494 Ack=772 Win=64765 Len=0
9120 52.007169   192.168.0.112     202.179.182.110   TCP     54 1876 → 80 [FIN, ACK] Seq=2494 Ack=772 Win=64765 Len=0
9121 52.011507   202.179.182.110   192.168.0.112     TCP     60 80 → 1876 [ACK] Seq=772 Ack=2495 Win=11680 Len=0
Referer: http://cafe.naver.com/common/flash/ajax.swf
x-flash-version: 10,2,152,26
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/6900A8C0-14D8BE9C000; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: lm4.cafe.naver.com
Connection: Keep-Alive
Cookie: NB=GM2DONZWG44TKMRQ; npic=dyb+QrPn8zzosEH9ET5IBsuEXYo4ZmobiLkc0rzdHbxmKlMogUMlVjKSpRemoX2/CA==; NNB=7ZKKAGURZSBE2; DA_HC=LZ11530540,LA; nid_inf=ed622106ba99c753d824f3c8678a8c05f3b847c6a123ea
ef4beea520ba0f5b01f100a6b51e92b1decb5a27ca08b63b1eadd8bcc4b63bd7912ce4e39547993e56053f31705ea8d039d84359ac37e67098f330519b37acf3ba510887030fdaa9e230027c5ebf512d775e1249f4ce9a697b; nid_pwa=2; NID_DH_
UI=0; NID_CNFG=4; NID_AUT=kOwrqV1WtD+BYycbQqo0TDKU1EWjro5UJt9TccfgZT1VNV1zndhpO7jYQt+J91vVgDSVwLowagL1tgl3Msgc2Fd5tUCIUvG35f4HntMXp97Obv+WKtp2x3L0OI8PwU4nd2avuVt7Ccca60uMvzyEEhen2symVnCnuvdByz3Qt2HB
Rc/eyJJau3sp/GX8ZxraXEIIIWGiNyrJKGYyTtnvENyqmiSIt+dHidoRqLheqKm9U3o8iThdqm4dLOOmccvSGgc+TiQ5OOL60d7mfRs1vsn59RvJOnsfQUGJpwr6XutV/oETksLfp75Cqs/N6AZJp4GprpiwMdanr2okRgxN9pJtbbpjyfQuGNtGgLHxpSU+jkaZyK
uG3/OoE62KYe4z+1OYglBmT09EVAnQXeTjmpENjAhboYJxtP1n7ycfDl8QXfoeW1DQkz3xIZcmIBAp5YTjh0xS0xiVqH+VSIG5JQBwiOwZlRxffHOb8K+QN1/sMB0jWdWK+8hVfm92xr4vw6VaZTPgmvq/TRHp/h2jLhE7HOcoj1rdnmPBCF4PwISq+vCCg41fzzcF
LlADjbeFWOTAIb2lKf0rcUn23eK73A==; NID_SES=6ONZYDjH/oAeQPeqZPn56BIKTEThKzNYajeGqK3zQycr/jCLatLm1SEhVGKsvam5; ncvid=#vid#_124.137.11.1345wyi; ncvc2=cefb1e3f242153e0cf2a4e7f4fa4c6a21f53ae4b1045a5738838
0bfb64778b428f67b53de4d84e671186df0ba71e8264b899bcac47701913; ncu=bc896c4d563f5ecac717cb89bc4cf5; nci4=3401e1cdde9ffa4211ffb8afa249255ad9855d99fc6c8f54defa9c5ce3d632e032df5578b5f96a4332d18a2cd1c54a9
46d7b4f5eb687e0ead635b559a89623c58abbf6878ea98cbd958d80a787b4e5e29393b691a6e99a958cab98d0a2ad86a697a506; ncmc4=6055b5998acbae1645abecfbf60f750ea6fc21cdbecc1de702c8d323aaae54937abc56d6122ec6e4b40e6db
142ad61d4422d4817b8c4e482f875970ff3cc51b7eedfd2ddfcdbe8a754; personaconmain|aackc=AE8BC98FD74D619F34FF891630DB0EFA0AECE715A6D7ED871B271CF74657399C; personacon|aackc=DB0D696415C6C1E5629524FB6C2F439FF
77975411ACCC02B107341C3BA38426063630C9A27E457B3; JSESSIONID=CEA92113FB9E20C0D83B531F9B0E4816


HTTP/1.1 200 OK
Date: Tue, 29 Mar 2011 10:00:47 GMT
Server: Apache/2.2.11 (Unix) mod_jk/1.2.27
Cache-Control: no-cache,no-store,must-revalidate
Pragma: no-cache
Expires: Wed, 31 Dec 1969 23:59:59 GMT
P3P: CP="ALL CURa ADMa DEVa TAIa OUR BUS IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC OTC"
Content-Length: 371
Connection: close
Content-Type: text/plain;charset=utf-8

{"c":"6","i":"http://itemimgs.naver.com/personacon","l":[
          {"m":"aackc","n":"......","p":"/94/63/2726394.gif"},
          {"m":"soseaz","n":"soseaz","p":"N"},
          {"m":"nig0412","n":"nig0412","p":"N"},
          {"m":"doochiri","n":".........","p":"/10/59/1015910.gif"},
          {"m":"hyouks74","n":"............","p":"/81/52/2525281.gif"},
          {"m":"katro","n":".........","p":"/27/84/1108427.gif"}
]}
```

네이버 카페 접속 기록

결론

192.168.0.112에서 192.168.0.15 이메일 서버에 여러 SYN 패킷과 RST 응답이 반복적으로 발생하고 있고 공격자는 SYN 패킷을 보내 열려 있는 포트를 찾고 있는 것으로 보인다.

파일에서 보낸 ICMP는 Neighbor Solicitation(NS) 메시지, IPv6 환경에서 네트워크 이웃의 MAC 주소를 확인하거나 새로 연결된 장치가 네트워크에 있는지 확인하기 위해 사용

HTTP GET 요청을 통해 /nateon/ticker 경로에 데이터를 요청
서버 응답 코드 200 OK가 반환되었으며, 이는 요청이 성공적으로 처리되었음을 의미
데이터 요청 시 쿠키 값이 포함된 것으로 보아, 사용자 인증 또는 개인화된 설정이 포함되었을 가능성이 있음
요청된 데이터는 NateOn에서 제공하는 뉴스 티커 서비스와 관련된 내용으로 보임

포트 스캐닝 중 SYN 패킷을 보냈을 때 SYN-ACK를 받으면, 이는 해당 포트가 열려 있음을 의미 (SYN -보내기, SYN-ACK -응답 받음(포트열림), ACK -보내 핸드셰이크 완료)