

1	0.000000	ASUSTekCOMPU. Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
2	0.068491	ASUSTekCOMPU. Broadcast	ARP	60	Who has 124.137.25.2? Tell 124.137.25.254
3	0.095860	fe80::8d87:2... ff02::c	SSDP	179	M-SEARCH * HTTP/1.1
4	0.096496	124.137.25.79 239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
5	0.097157	fe80::8d87:2... ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
6	0.097162	124.137.25.79 239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
7	0.620765	fe80::f9c3:c... ff02::1:ff35:5...	ICMPv6	86	Neighbor Solicitation for fe80::8468:9951:be35:5962 from a4:ba:db:52:13:07
8	2.869813	124.137.25.20 168.126.63.1	DNS	76	Standard query 0x6369 A www.google.co.kr
9	2.877339	168.126.63.1 124.137.25.20	DNS	292	Standard query response 0x6369 A www.google.co.kr CNAME www.google.com CNAME www.l.google.com
10	2.884835	124.137.25.20 66.249.89.104	TCP	78	2818 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
11	3.002552	66.249.89.104 124.137.25.20	TCP	66	80 → 2818 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
12	3.003517	124.137.25.20 66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=1 Ack=1 Win=263120 Len=0
13	3.003536	124.137.25.20 66.249.89.104	HTTP	621	GET / HTTP/1.1
14	3.096004	124.137.25.79 239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	3.096330	fe80::8d87:2... ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
16	3.096745	fe80::8d87:2... ff02::c	SSDP	179	M-SEARCH * HTTP/1.1
17	3.096751	124.137.25.79 239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
18	3.121003	66.249.89.104 124.137.25.20	TCP	60	80 → 2818 [ACK] Seq=1 Ack=568 Win=6912 Len=0
19	3.161806	66.249.89.104 124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=1 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
20	3.161834	66.249.89.104 124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=1431 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
21	3.161847	66.249.89.104 124.137.25.20	TCP	1098	80 → 2818 [PSH, ACK] Seq=2861 Ack=568 Win=6912 Len=1044 [TCP PDU reassembled in 33]
22	3.161859	66.249.89.104 124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=3905 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
23	3.161872	66.249.89.104 124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=5335 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
24	3.161886	66.249.89.104 124.137.25.20	TCP	1290	80 → 2818 [PSH, ACK] Seq=6765 Ack=568 Win=6912 Len=1236 [TCP PDU reassembled in 33]
25	3.162009	124.137.25.20 66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=568 Ack=2861 Win=263120 Len=0
26	3.162023	124.137.25.20 66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=568 Ack=3905 Win=262072 Len=0
27	3.162029	124.137.25.20 66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=568 Ack=6765 Win=263120 Len=0
28	3.162035	124.137.25.20 66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=568 Ack=8001 Win=261880 Len=0
29	3.162089	66.249.89.104 124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=8001 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
30	3.162102	66.249.89.104 124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=9431 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
31	3.162111	66.249.89.104 124.137.25.20	TCP	346	80 → 2818 [PSH, ACK] Seq=10861 Ack=568 Win=6912 Len=292 [TCP PDU reassembled in 33]

no. 1, 2

- ARP 요청으로, 장치가 특정 IP 주소(124.137.25.219, 124.137.25.2)에 해당하는 MAC 주소를 탐색 -> 124.137.25.254 확인

no. 3~6, 14~17

- UPnP 장치 검색 활동으로, 네트워크에 연결된 장치(예: IoT 장치, 스마트 TV 등)를 탐색하려는 시도

no. 7

- Neighbor Solicitation 메시지를 통해 IPv6 네트워크에서 특정 링크-로컬 주소의 장치 탐색을 시도

no. 8~9

- DNS 질의: google.co.kr에 대한 질의가 발생
- DNS 응답: Google 서버의 IP 주소가 반환됨
- 사용자가 Google 도메인에 접속하려고 시도했으며, DNS 요청 및 응답은 정상적으로 처리됨
- DNS 응답에는 필요한 정보(CNAME(별칭), A 레코드, NS 레코드)가 포함되어 있으며, Google 도메인으로 정상적으로 매핑
- DNS 서버 IP(168.126.63.1)는 한국 통신사의 공용 DNS 서버

no. 10~12

- TCP 3-way handshake : 클라이언트와 Google 서버 간에 정상적인 TCP 연결이 설정

no. 13~32

- HTTP GET 요청: Google 서버(66.249.89.104)로 전송됨
- PSH, ACK 플래그가 사용되어 데이터를 즉시 전송함
- 사용자가 Google 서버와 HTTP를 통해 데이터를 교환

30	3.162102	66.249.89.104	124.137.25.20	TCP	1484	80 → 2818 [ACK] Seq=9431 Ack=568 Win=6912 Len=1430 [TCP PDU reassembled in 33]
31	3.162111	66.249.89.104	124.137.25.20	TCP	346	80 → 2818 [PSH, ACK] Seq=10861 Ack=568 Win=6912 Len=292 [TCP PDU reassembled in 33]
32	3.162204	124.137.25.20	66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=568 Ack=10861 Win=263120 Len=0
33	3.162356	66.249.89.104	124.137.25.20	HTTP	1385	HTTP/1.1 200 OK (text/html)
34	3.162414	124.137.25.20	66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=568 Ack=12484 Win=261496 Len=0
35	3.163081	124.137.25.20	66.249.89.104	TCP	54	[TCP Window Update] 2818 → 80 [ACK] Seq=568 Ack=12484 Win=263120 Len=0
36	3.230370	124.137.25.20	66.249.89.104	HTTP	750	GET /ig/f/qXu29BUALEY/intl/ALL_kr/homepage_v3.css HTTP/1.1
37	3.557274	66.249.89.104	124.137.25.20	HTTP	155	404 Not Modified
38	3.528670	124.137.25.20	168.126.63.1	DNS	75	Standard query 0xcafd A id.google.co.kr
39	3.532855	124.137.25.20	66.249.89.104	TCP	54	2818 → 80 [ACK] Seq=1264 Ack=12615 Win=262984 Len=0
40	3.533398	168.126.63.1	124.137.25.20	DNS	336	Standard query response 0xcafd A id.google.co.kr CNAME id.1.google.com A 64.233.183.139 A 64.233.183.100 A 64.233.183.101 A 64.233.183.102
41	3.535449	124.137.25.20	64.233.183.139	TCP	78	2819 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
42	3.581538	124.137.25.20	74.125.155.101	TCP	78	2820 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
43	3.611319	124.137.25.20	64.233.183.138	TCP	78	2821 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
44	3.626079	64.233.183.1..	124.137.25.20	TCP	66	80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
45	3.693258	64.233.183.1..	124.137.25.20	TCP	66	80 → 2821 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
46	3.694294	124.137.25.20	64.233.183.138	TCP	54	2821 → 80 [ACK] Seq=1 Ack=1 Win=263120 Len=0
47	3.694316	124.137.25.20	64.233.183.138	HTTP	673	GET /generate_204 HTTP/1.1
48	3.776837	64.233.183.1..	124.137.25.20	TCP	60	80 → 2821 [ACK] Seq=1 Ack=620 Win=6976 Len=0
49	3.776862	64.233.183.1..	124.137.25.20	HTTP	179	HTTP/1.1 204 No Content
50	3.786011	74.125.155.1..	124.137.25.20	TCP	66	80 → 2820 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
51	3.787099	124.137.25.20	74.125.155.101	TCP	54	2820 → 80 [ACK] Seq=1 Ack=1 Win=263120 Len=0
52	3.787116	124.137.25.20	74.125.155.101	HTTP	465	GET /csi?v=3&as=uehph_kr&action=&e=17259&et=ol.344,prt.359 HTTP/1.1
53	3.846967	ASUSTekCOMPU..	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
54	3.978401	124.137.25.20	64.233.183.138	TCP	54	2821 → 80 [ACK] Seq=620 Ack=126 Win=262992 Len=0
55	3.981655	64.233.183.1..	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
56	3.991975	74.125.155.1..	124.137.25.20	TCP	60	80 → 2820 [ACK] Seq=1 Ack=412 Win=5848 Len=0
57	4.012119	ASUSTekCOMPU..	Broadcast	ARP	60	Who has 124.137.25.73? Tell 124.137.25.254
58	4.072348	74.125.155.1..	124.137.25.20	HTTP	269	HTTP/1.1 204 No Content
59	4.189183	124.137.25.20	74.125.155.101	TCP	54	2820 → 80 [ACK] Seq=412 Ack=216 Win=262904 Len=0

no. 33

- HTTP 1.1을 사용하여 통신
- 200 OK 응답: 요청한 리소스(HTML 또는 기타 웹 콘텐츠)가 정상적으로 전송됨

no. 35

- Window Update: TCP 윈도우 크기를 업데이트하여 송신자가 전송 가능한 데이터의 양을 조정
- TCP Window Update는 주로 대규모 데이터 전송 중에 발생하며, 네트워크에서 자주 볼 수 있는 패킷 유형

no. 36

- 클라이언트는 Google 서버에서 CSS 파일을 요청했으며, 이는 웹페이지 렌더링을 위한 정상적인 HTTP GET 요청
- Google 웹페이지 리소스를 요청하는 것으로 보아 사용자가 브라우저에서 Google 웹사이트를 탐색 중일 가능성
- CSS 파일은 웹페이지의 스타일(레이아웃, 글꼴 등)을 정의하는데 사용
- URL 경로: /ig/f/qXu29BUALEY/intl/ALL_kr/homepage_v3.css

no. 37

- 304 Not Modified: 요청한 리소스(homepage_v3.css)가 이전 요청 이후로 변경되지 않았음을 나타냄
- 304 Not Modified 응답은 네트워크 효율성을 높이고, 클라이언트가 캐시된 데이터를 사용하도록 지시함

no. 38, 40

- 질의 도메인: id.google.co.kr
- 0xcafd: 클라이언트가 보낸 질의와 응답을 매칭하는 고유 식별자
- 응답 유형: A(IPv4) 및 CNAME(별칭), NS(Name Server)
- 정상적인 DNS 응답으로, 클라이언트가 id.google.co.kr 도메인과 통신하기 위한 IP 주소를 얻는 데 사용
- 반환된 정보는 Google의 글로벌 서버와 연결할 수 있도록 설계된 것으로 추정

no. 47

- 클라이언트가 Google 서버에 /generate_204를 요청하여 연결 상태를 점검하거나 네트워크 상태를 확인하기 위한 것
- URL 경로: /generate_204

no. 49, 58

- 204 No Content : 요청이 성공적으로 처리되었지만, 서버는 클라이언트로 반환할 본문 데이터가 없음을 나타냄

no. 52

- URL 경로: /csi?v=3&s=webhp_kr&action=&e=17259&rt=ol.344,prt.359
- 파라미터 분석:
 - v=3: 버전 정보 (버전 3)
 - s=webhp_kr: 서비스 또는 섹션(webhp, 한국 지역) 식별자
 - action=: 특정 이벤트나 작업(미정의 상태)
 - e=17259: 이벤트 ID 또는 상태 코드
 - rt=ol.344,prt.359: 성능 측정값:
 - ol.344: 페이지 로드 완료 시간
 - prt.359: 페이지 렌더링 완료 시간
- Google 서비스에서 페이지 성능 및 사용자 이벤트 데이터를 수집하기 위해 클라이언트가 서버로 전송한 HTTP GET 요청

no. 53, 57

- ARP 요청으로, 장치가 특정 IP 주소(124.137.25.67, 124.137.25.73)에 해당하는 MAC 주소를 탐색 -> 124.137.25.254 확인

no. 55

- TCP Retransmission : TCP 재전송

no. 60~62, 111, 166(rst)

59	4.189183	124.137.25.20	74.125.155.101	TCP	54	2820 → 80 [ACK] Seq=412 Ack=216 Win=262904 Len=0
60	4.413619	124.137.25.20	66.249.89.104	TCP	54	2818 → 80 [RST, ACK] Seq=1264 Ack=12615 Win=0 Len=0
61	4.413645	124.137.25.20	74.125.155.101	TCP	54	2820 → 80 [RST, ACK] Seq=412 Ack=216 Win=0 Len=0
62	4.413654	124.137.25.20	64.233.183.138	TCP	54	2821 → 80 [RST, ACK] Seq=620 Ack=126 Win=0 Len=0
63	4.581849	64.233.183.138	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
64	4.839259	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
65	5.008765	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.73? Tell 124.137.25.254
66	5.781577	64.233.183.138	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
67	5.838837	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
68	6.008840	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.73? Tell 124.137.25.254
69	6.021552	124.137.25.20	89.16.178.151	TCP	78	2822 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
70	6.340374	89.16.178.151	124.137.25.20	TCP	66	80 → 2822 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
71	6.341338	124.137.25.20	89.16.178.151	TCP	54	2822 → 80 [ACK] Seq=1 Ack=1 Win=262800 Len=0
72	6.341351	124.137.25.20	89.16.178.151	HTTP	598	GET /bb5eafbc6c6e67e11c4afc88b4e1dd22/testcase.html HTTP/1.1
73	6.649843	89.16.178.151	124.137.25.20	TCP	60	80 → 2822 [ACK] Seq=1 Ack=545 Win=7040 Len=0
74	6.649867	89.16.178.151	124.137.25.20	HTTP	192	HTTP/1.1 304 Not Modified
75	6.770385	124.137.25.20	89.16.178.151	TCP	54	2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
76	6.772458	124.137.25.20	89.16.178.151	TCP	78	2826 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
77	6.814347	124.137.25.20	89.16.178.151	TCP	54	2822 → 80 [ACK] Seq=545 Ack=139 Win=262656 Len=0
78	6.938654	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
79	7.012446	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.73? Tell 124.137.25.254
80	7.067262	89.16.178.151	124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
81	7.068893	89.16.178.151	124.137.25.20	TCP	66	80 → 2826 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
82	7.069158	124.137.25.20	89.16.178.151	TCP	54	2826 → 80 [ACK] Seq=1 Ack=1 Win=262800 Len=0
83	7.069337	124.137.25.20	89.16.178.151	HTTP	208	OPTIONS / HTTP/1.1
84	7.367107	89.16.178.151	124.137.25.20	TCP	60	80 → 2826 [ACK] Seq=1 Ack=155 Win=6912 Len=0
85	7.367679	89.16.178.151	124.137.25.20	HTTP	262	HTTP/1.1 200 OK
86	7.369112	124.137.25.20	89.16.178.151	HTTP	227	PROPFIND /calc.jar HTTP/1.1
87	7.494259	51.80.05:66	Broadcast	ARP	64	ARP Announcement for 124.137.25.4
88	7.680313	89.16.178.151	124.137.25.20	HTTP/XML	1151	HTTP/1.1 207 Multi-Status
89	7.682223	124.137.25.20	89.16.178.151	HTTP	227	PROPFIND /calc.jar HTTP/1.1

- 클라이언트가 서버와의 연결을 재설정(강제 종료)함

- 연결 설정 실패 또는 시간 초과로 인해 클라이언트가 연결을 종료

no. 63, 66, 95, 99, 113, 115

- TCP Retransmission : 재전송

- 네트워크 지연, 패킷 손실, 또는 서버의 응답 대기 초과로 발생

no. 65, 67~68, 78~79

- 브로드캐스트

no. 72

- 클라이언트가 특정 HTML 파일(testcase.html)을 요청했으며, 이 요청은 웹 테스트, 실험, 또는 특정 페이지 로드와 관련

- URL 경로에 랜덤 문자열(/bb5eafbc6c6e67e11c4afc88b4e1dd22)이 포함되어 있어, 자동화된 봇 또는 스크립트에서 생성된 요청일 가능성도 있음

- 요청이 의도된 테스트 또는 설정이 아닌 경우, 서버에서 의심스러운 트래픽으로 간주될 가능성이 있음

- 요청 자체는 정상적인 HTTP GET 요청으로 보이지만 요청 URL의 경로가 랜덤 문자열로 보이는 점에서 봇 트래픽 또는 테스트 시나리오일 가능성을 배제할 수 없음

no. 74

- 304 Not Modified: 요청한 리소스가 이전 요청 이후로 변경되지 않았음을 나타냄

no. 80, 102, 118, 161

- ICMP 메시지 유형:

Type: 3 (Destination Unreachable)

Code: 10 (Host administratively prohibited)

서버 또는 네트워크가 관리 정책(방화벽 설정)에 따라 클라이언트의 요청을 차단했음을 의미

no. 83

- 클라이언트가 서버의 루트 경로에 대해 OPTIONS 요청을 보냄
- 요청은 서버에서 지원하는 HTTP 메소드를 확인하려는 용도

no. 85

- 200 OK : 요청이 성공적으로 처리되었음을 나타냄. / OPTIONS 요청에 대한 정상적인 응답

no. 86, 89, 93

- PROPFIND:

클라이언트가 서버에서 리소스(/calc.jar)의 속성을 요청

WebDAV에서 주로 사용되며, 파일 및 디렉토리의 메타데이터(예: 파일 크기, 생성일, 수정일 등)를 반환받기 위해 사용

- 클라이언트가 /calc.jar에 대한 속성 정보를 요청하는 WebDAV 요청(PROPFIND)을 전송
- 요청은 WebDAV 기능이 활성화된 서버에서 정상적일 수 있지만, 의도되지 않은 활동일 경우 의심스러운 탐색 또는 스캐닝 활동일 가능성도 있음

no. 88, 92

- 207 Multi-Status:

WebDAV에서 사용되며, 요청된 리소스에 대해 여러 응답 상태를 포함

일반적으로 XML 포맷으로 여러 리소스 또는 속성에 대한 상태 정보를 제공

90	7.813038	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
91	7.928885	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
92	7.998611	89.16.178.151 124.137.25.20	HTTP/XML	1151	HTTP/1.1 207 Multi-Status
93	8.000127	124.137.25.20 89.16.178.151	HTTP	261	GET /calc.jar HTTP/1.1
94	8.008917	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.73? Tell 124.137.25.254
95	8.181955	64.233.183.1 124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
96	8.305750	89.16.178.151 124.137.25.20	HTTP	191	HTTP/1.1 304 Not Modified
97	8.565417	124.137.25.20 89.16.178.151	TCP	54	2826 → 80 [ACK] Seq=708 Ack=2540 Win=262656 Len=0
98	8.809751	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
99	8.892771	124.137.25.20 89.16.178.151	TCP	54	[TCP Retransmission] 2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
100	8.928966	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
101	9.009086	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.73? Tell 124.137.25.254
102	9.206777	89.16.178.151 124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
103	9.458710	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.2? Tell 124.137.25.254
104	9.800423	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.34? Tell 124.137.25.254
105	9.809008	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
106	10.449409	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.2? Tell 124.137.25.254
107	10.799106	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.34? Tell 124.137.25.254
108	11.449113	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.2? Tell 124.137.25.254
109	11.642052	89.16.178.151 124.137.25.20	TCP	60	80 → 2822 [FIN, ACK] Seq=139 Ack=545 Win=7040 Len=0
110	11.642640	124.137.25.20 89.16.178.151	TCP	54	2822 → 80 [ACK] Seq=545 Ack=140 Win=262656 Len=0
111	11.643029	124.137.25.20 89.16.178.151	TCP	54	2822 → 80 [RST, ACK] Seq=545 Ack=140 Win=0 Len=0
112	11.799620	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.34? Tell 124.137.25.254
113	12.382209	64.233.183.1 124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
114	13.047099	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.34? Tell 124.137.25.254
115	13.168357	124.137.25.20 89.16.178.151	TCP	54	[TCP Retransmission] 2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
116	13.298779	89.16.178.151 124.137.25.20	TCP	60	80 → 2826 [FIN, ACK] Seq=2540 Ack=708 Win=10240 Len=0
117	13.299103	124.137.25.20 89.16.178.151	TCP	54	2826 → 80 [ACK] Seq=708 Ack=2541 Win=262656 Len=0
118	13.462395	89.16.178.151 124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
119	13.672553	124.137.25.2 124.137.25.255	BROWSER	243	Host Announcement CANONAG2FFD, Workstation, Server, Print Queue Server
120	14.039914	ASUSTekCOMPU.. Broadcast	ARP	60	Who has 124.137.25.34? Tell 124.137.25.254

no. 90, 92, 94, 98, 103~108, 112, 114, 120

- ARP 요청으로, 장치가 특정 IP 주소에 해당하는 MAC 주소를 탐색

no. 119

- 프로토콜 : BROWSER (NetBIOS 기반)
- 호스트 이름: CANONAG2FFD
- 서비스 역할:

Workstation: 일반 사용자 작업 스테이션 역할

Server: 네트워크 리소스를 제공하는 서버 역할

Print Queue Server: 네트워크 프린터 큐를 제공

- Host Announcement 메시지는 NetBIOS 기반 네트워크에서 흔히 발생하며, 네트워크 브라우저(예: Windows 네트워크 탐색기)에서 장치를 표시하는 데 사용됨
- CANONA62FFD라는 이름으로 보아, Canon 프린터 또는 다기능 장치에서 생성된 메시지일 가능성이 큼

121	14.478579	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
122	15.039315	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.34? Tell 124.137.25.254
123	15.469350	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
124	16.034715	124.137.25.20	89.16.178.151	TCP	78	2827 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
125	16.237643	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.198? Tell 124.137.25.222
126	16.353828	89.16.178.151	124.137.25.20	TCP	66	80 → 2827 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
127	16.354421	124.137.25.20	89.16.178.151	TCP	54	2827 → 80 [ACK] Seq=1 Ack=1 Win=262800 Len=0
128	16.354665	124.137.25.20	89.16.178.151	HTTP	657	GET /calc.jar HTTP/1.1
129	16.387940	124.137.25.20	168.126.63.1	DNS	82	Standard query 0xe206 A liveupdate.alyac.co.kr
130	16.398935	168.126.63.1	124.137.25.20	DNS	206	Standard query response 0xe206 A liveupdate.alyac.co.kr CNAME alyac.download.xcdnplus.co.kr A 121.156.106.5 NS gtm2.xcdnplus.co.kr NS g
131	16.469429	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.67? Tell 124.137.25.254
132	16.653110	89.16.178.151	124.137.25.20	TCP	60	80 → 2827 [ACK] Seq=1 Ack=604 Win=7168 Len=0
133	16.654234	89.16.178.151	124.137.25.20	HTTP	1074	HTTP/1.1 200 OK (application/x-java-archive)
134	16.877511	124.137.25.20	89.16.178.151	TCP	54	2827 → 80 [ACK] Seq=604 Ack=1021 Win=261776 Len=0
135	17.206170	ASUSTekCOMPU...	Broadcast	IPX SAP	113	General broadcast
136	17.919440	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.198? Tell 124.137.25.223
137	18.168815	124.137.25.20	202.179.182.110	TCP	78	2829 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM
138	18.164149	202.179.182...	124.137.25.20	TCP	60	80 → 2829 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
139	18.164262	124.137.25.20	202.179.182.110	TCP	54	2829 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
140	18.168247	202.179.182...	124.137.25.20	TCP	60	[TCP ACKed unseen segment] 80 → 2829 [ACK] Seq=1 Ack=1461 Win=8768 Len=0
141	18.168267	202.179.182...	124.137.25.20	TCP	60	[TCP ACKed unseen segment] 80 → 2829 [ACK] Seq=1 Ack=2494 Win=11680 Len=0
142	18.169305	202.179.182...	124.137.25.20	HTTP	936	HTTP/1.1 200 OK (text/plain)
143	18.169320	202.179.182...	124.137.25.20	TCP	60	80 → 2829 [FIN, ACK] Seq=883 Ack=2494 Win=11680 Len=0
144	18.169259	124.137.25.20	202.179.182.110	TCP	54	[TCP ACKed unseen segment] 80 → 2829 [ACK] Seq=2494 Ack=884 Win=64653 Len=0
145	18.170461	124.137.25.20	202.179.182.110	TCP	54	2829 → 80 [FIN, ACK] Seq=2494 Ack=884 Win=64653 Len=0
146	18.173494	202.179.182...	124.137.25.20	TCP	60	80 → 2829 [ACK] Seq=884 Ack=2495 Win=11680 Len=0
147	18.436736	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
148	18.916158	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
149	19.429836	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.122? Tell 124.137.25.254
150	19.575269	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.2? Tell 124.137.25.254
151	19.989525	ASUSTekCOMPU...	Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254

no. 128

- /calc.jar: .jar 확장자를 가진 Java 애플리케이션 아카이브 파일
- Java 애플리케이션을 실행하거나 특정 기능을 제공하는 데 사용
- 클라이언트는 서버에서 /calc.jar라는 Java Archive 파일을 요청하는 HTTP GET 요청을 전송

no. 129, 130

- 쿼리 ID: 0xe206 (요청과 응답을 매칭하는 고유 식별자)
- 클라이언트는 보안 소프트웨어 업데이트를 위해 liveupdate.alyac.co.kr의 IPv4 주소를 확인하는 정상적인 DNS 요청을 전송
- DNS 서버는 클라이언트 요청에 대해 liveupdate.alyac.co.kr의 CNAME 및 IPv4 주소를 반환
- CNAME (Canonical Name) 레코드:

alyac.download.xcdnplus.co.kr은 XCDN 서비스(콘텐츠 배포 네트워크)를 통해 제공되는 도메인으로, 빠르고 안정적인 콘텐츠 배포를 위해 사용됨

- NS (Name Server) 레코드:

XCDN 서비스 도메인(xcdnplus.co.kr)을 관리하는 네임 서버:

gtm2.xcdnplus.co.kr: 121.254.225.2

gtm1.xcdnplus.co.kr: 121.156.106.2

no. 133

- 서버는 클라이언트 요청에 따라 Java Archive 파일(application/x-java-archive)을 반환

no. 135

- IPX SAP (Service Advertising Protocol):

Novell NetWare 환경에서 주로 사용되며, 네트워크에서 특정 서비스(예: 파일 서버, 프린터

서버 등)를 광고하거나 위치를 알리는 데 사용

-General Response:

네트워크 상의 다른 장치가 요청한 서비스의 정보를 반환하거나, 주기적으로 자신의 서비스 정보를 광고

- SAP 메시지는 일반적으로 다음 정보를 포함

서비스 유형: 서비스 유형(예: 파일 서버, 프린터 서버, 기타 애플리케이션 서비스)을 나타냄

네트워크 주소: 서비스가 위치한 네트워크의 주소 정보(IPX 네트워크 ID 포함)

노드 및 소켓: 서비스가 실행 중인 장치의 노드 및 소켓 정보

- SAP General Response 메시지로, IPX 프로토콜을 통해 네트워크에서 특정 서비스를 광고하거나 응답

no. 140,141

- [TCP ACKed unseen segment] : 패킷 손실 또는 캡처되지 않은 데이터 세그먼트를 나타냄

no. 142

- text/plain 콘텐츠는 로그 파일, 단순한 텍스트 메시지 등 다양한 데이터를 반환

- 서버(202.179.182.110)는 클라이언트(124.137.25.20)의 요청에 대해 HTTP/1.1 200 OK 상태 코드와 함께 텍스트 데이터를 반환

no. 144

- [TCP Previous segment not captured] : 이전에 클라이언트 또는 서버가 전송한 TCP 세그먼트를 캡처하지 못했음을 나타냄

147	18.916158	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
148	18.916158	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
149	19.429836	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
150	19.429836	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
151	19.909525	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
152	20.429607	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
153	20.569609	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
154	20.910810	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
155	21.349948	ASUSTekCOMPU... SamsungElect_b...	ARP	60	Who has 124.137.25.20? Tell 124.137.25.254
156	21.350254	SamsungElect... ASUSTekCOMPU_4...	ARP	42	124.137.25.20 is at 00:13:77:bd:2d:5c
157	21.569696	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
158	21.581110	124.137.25.20 89.16.178.151	TCP	54	[TCP Retransmission] 2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
159	21.677184	89.16.178.151 124.137.25.20	TCP	60	80 → 2827 [FIN, ACK] Seq=1021 Ack=604 Win=7168 Len=0
160	21.677784	124.137.25.20 89.16.178.151	TCP	54	2827 → 80 [ACK] Seq=604 Ack=1022 Win=261776 Len=0
161	21.892604	89.16.178.151 124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
162	21.927389	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
163	22.126797	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
164	22.919974	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
165	23.119750	ASUSTekCOMPU... Broadcast	ARP	60	Who has 124.137.25.219? Tell 124.137.25.254
166	23.159668	124.137.25.20 89.16.178.151	TCP	54	2827 → 80 [RST, ACK] Seq=604 Ack=1022 Win=0 Len=0

no. 156

- IP 주소 124.137.25.20는 물리적 주소 00:13:77:bd:2d:5c와 연결되어 있음을 나타냄

75	6.770385	124.137.25.20	89.16.178.151	TCP	54	2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
80	7.067262	89.16.178.151	124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
99	8.892771	124.137.25.20	89.16.178.151	TCP	54	[TCP Retransmission] 2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
102	9.206777	89.16.178.151	124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
115	13.160357	124.137.25.20	89.16.178.151	TCP	54	[TCP Retransmission] 2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
118	13.462395	89.16.178.151	124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)
158	21.581110	124.137.25.20	89.16.178.151	TCP	54	[TCP Retransmission] 2812 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32832 Len=0
161	21.892604	89.16.178.151	124.137.25.20	ICMP	82	Destination unreachable (Host administratively prohibited)

- 클라이언트가 TCP 세션을 정상적으로 종료하려 했으나, 서버나 중간 네트워크 장치의 관리 정책에 의해 차단
- ICMP "Destination Unreachable (Host administratively prohibited)" 메시지는 방화벽이나 네트워크 정책에 의해 발생했을 가능성이 높음

41	3.535440	124.137.25.20	64.233.183.139	TCP	78	2819 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 SACK_PERM
44	3.626070	64.233.183.1..	124.137.25.20	TCP	66	80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
55	3.981663	64.233.183.1..	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
63	4.581849	64.233.183.1..	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
66	5.781577	64.233.183.1..	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
95	8.181955	64.233.183.1..	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64
113	12.982289	64.233.183.1..	124.137.25.20	TCP	66	[TCP Retransmission] 80 → 2819 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PERM WS=64

- 서버는 클라이언트로부터 TCP 연결의 마지막 단계(ACK)를 받지 못하고 지속적으로 SYN, ACK를 재전송
- 네트워크 패킷 손실, 클라이언트 응답 누락, 또는 방화벽/보안 장치의 차단 가능성


```
GET /csi?v=3&s=webhp_kr&action=&e=17259&rt=ol.344,prt.359 HTTP/1.1
Accept: */*
Referer: http://www.google.co.kr/
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/1419897C-14C4645E2C2-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: csi.gstatic.com
Connection: Keep-Alive

HTTP/1.1 204 No Content
Content-Length: 0
Date: Wed, 21 Jan 2004 19:51:30 GMT
Pragma: no-cache
Cache-Control: private, no-cache
Expires: Wed, 17 Sep 1975 21:32:10 GMT
Content-Type: text/html
Server: Golfe
```

Accept: 모든 데이터 형식을 허용 (*/*)

Referer: 요청이 <http://www.google.co.kr/>에서 시작되었음을 나타낸다

Accept-Encoding: 콘텐츠 인코딩을 gzip 또는 deflate로 허용

User-Agent: 클라이언트는 Internet Explorer 7.0, Windows XP 기반으로 동작.

Host: 요청 대상 서버: csi.gstatic.com

Connection: 연결 유지(Keep-Alive)로 설정

204 No Content: 요청은 성공적으로 처리되었으나, 응답 Content 없음

Cache-Control: 응답은 개인용으로만 캐싱이 가능하며, 캐시되지 않아야 함

Expires: 응답 만료 시간이 과거로 설정됨(캐시 비활성화 의도)

Server: 서버 정보가 Golfe

클라이언트가 csi.gstatic.com 서버에 GET /csi 요청을 보내고 있음.

csi는 일반적으로 Google이 사용하는 "Client Side Instrumentation"의 약어, 사용자 동작을 로깅하거나 성능 데이터 수집하기 위한 요청일 가능성이 큼.

rt 파라미터에서 로드 타임(ol.344, prt.359)이 포함되어 있어 성능 로깅이 의도된 것으로 추정.

응답이 204 No Content, 서버는 요청을 성공적으로 처리했으나 별도의 응답 데이터는 반환하지 않음.

로깅 요청(사용자 추적, 성능 기록)에서 자주 발생하는 패턴.

시간 정보:

응답 날짜가 2004년으로 설정되어 있지만, 이는 실제 시간과 다를 가능성이 있음(시스템 설정 오류 또는 의도적인 빈 값 제공).

User-Agent 및 요청 헤더를 보아 오래된 브라우저 및 운영체제에서의 동작을 분석한 것일 수 있음.

```

GET /generate_204 HTTP/1.1
Accept: */*
Referer: http://www.google.co.kr/
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/1419897C-14C4645E2C2-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: clients1.google.co.kr
Connection: Keep-Alive
Cookie: PREF=ID=f740ee6473e4d08c:U=8b2018b6f27902d0:Nw=1:TM=1279679410:LM=1279679411:S=VxXrkgKtNptuI1B5; NID=37=c0W9nJrlekq2l_gopgdasnrJd9l1NEiJkrmuEX-mH9UJ_rBcDMpS_IDOX3AGAiHfcuJNyPswM4c4dd-0ymzd5pu30tDtG4w7Y80dabjgH2ij3u8vhguwHRBGLdnQuze

HTTP/1.1 204 No Content
Content-Length: 0
Content-Type: text/html
Date: Wed, 21 Jul 2010 02:33:22 GMT
Server: GFE/2.0

```

요청이 유입된 페이지는 <http://www.google.co.kr>

요청 대상 서버: clients1.google.co.kr

클라이언트는 Google 서비스와 관련된 쿠키를 포함하여 요청을 보냄

PREF: 사용자 기본 설정과 관련된 ID

NID: Google 서비스 인증 또는 추적 관련 쿠키

/generate_204는 Google 서비스에서 클라이언트와의 연결 상태를 확인하거나, 네트워크 상태를 점검하기 위한 목적으로 사용

브라우저 또는 Google 서비스 앱에서 주기적으로 실행될 가능성이 높음.

서버는 요청을 성공적으로 처리하였으며, 본문 없이 204 No Content 상태를 반환
응답 본문이 없으므로 서버와 클라이언트 간의 단순 연결 확인 작업에 적합.

```

GET /bb5eafbc6c6e7e11c4afc88b4e1dd22/testcase.html HTTP/1.1
Accept: */*
Referer: http://cafe.naver.com/ArticleRead.nhn?clubid=11633828&menuid=45&boardtype=L&page=2&userDisplay=&articleid=2513
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Fri, 09 Apr 2010 09:44:00 GMT
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/1419897C-14C4645E2C2-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: lock.cmpxchg8b.com
Connection: Keep-Alive

HTTP/1.1 304 Not Modified
Date: Wed, 21 Jul 2010 02:34:11 GMT
Server: Apache
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100

```

요청 경로: /05ebafbc6c6e7e11cdfc888bd1ed2d2/testcase.html

특정 파일 testcase.html 요청

Referer:

<http://cafe.naver.com/ArticleRead.nhn?clubid=11633828&menuid=45&boardtype=L&page=2&userDisplay=&articleid=251>: 요청이 유입된 페이지는 네이버 카페의 특정 게시글에서 발생, 게시글 ID는 251.

요청 대상 서버: lock.cmpxchg.com

상태 코드: 304 Not Modified (해당 콘텐츠를 요청하지 않고 자신의 로컬에 저장되어있는 캐시를 사용)

클라이언트가 요청한 리소스가 If-Modified-Since 이후로 수정되지 않았음을 의미

Keep-Alive: timeout=5, max=100

연결을 5초 동안 유지하며, 최대 100개의 요청을 처리 가능

클라이언트는 특정 테스트 파일(testcase.html)에 대한 요청을 보냄, 이 파일이 네이버 카페의 특정 게시글과 관련된 것으로 보임.

클라이언트는 이미 이 파일의 캐시를 보유하고 있으며, 변경 사항이 있을 경우에만 서버에서 새 데이터를 받으려 함(If-Modified-Since 헤더).

서버는 파일이 이전 요청 이후로 변경되지 않았음을 나타내는 304 Not Modified 상태를 반환.

```
GET /calc.jar HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/1419897C-14C4645E2C2-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: lock.cmpxchg8b.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 21 Jul 2010 02:34:21 GMT
Server: Apache
Last-Modified: Tue, 06 Apr 2010 23:13:18 GMT
Accept-Ranges: bytes
Content-Length: 761
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-java-archive

PK..
....X..<.....META-INF/...PK.....<.....META-INF/MANIFEST.MF.M..LK-..
K*....R0.3...M...u.I...R.y.x.PK..|.;*...+...PK...W.<.....
..Main.classMQM0.}.WaE...V.....7.....F...<.e.KhkJ1.-/j<...Q..j..4.y;og..I?...?.a.#...
V.X..n`..&C.Dy*<eH...C...K...<y9q{2.uz#b../.Q. ....T....a....(w ..j...=t..K.X....."u'.P}e.3.?.
..*.....O.!.v.i.....@..v.j...p.M9.uK.i@..y.b....4....7.".....2.b.f...%>....
..^<...9g.?.u..9..h.4...%...s.Y..0}.
..=s...b.b...p.0.%..J7.Gb..C..|A..V.....*E...tR.T.,G=.oPK..w..i_.....PK..
.
....X..<.....META-INF/...PK.....<|.j.*...+.....+...META-INF/MANIFEST.MFPK.....
.W..<w..i_.....
.....Main.classPK.....
```

JAR(Java Archive) 파일 calc.jar을 요청

application/x-java-archive는 JAR 파일을 다운로드할 수 있음을 나타냄

요청 대상 서버: lock.cmpxchg8b.com

200 OK: 요청한 리소스가 정상적으로 처리되었으며, 응답 본문에 JAR 파일이 포함되어 있음.

응답 데이터의 MIME 타입은 application/x-java-archive

파일 크기는 761바이트로 매우 작음

Last-Modified 헤더를 통해 파일의 마지막 수정 날짜가 제공됨.

```

HTTP/1.1 200 OK
Date: Wed, 21 Jul 2010 02:33:37 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: 483
Connection: close
Content-Type: text/plain;charset=utf-8

{"c": "9", "i": "http://itemings.naver.com/personacon", "l": [
  {"m": "aackc", "n": ".....", "p": "/94/63/s_2726394.gif"},
  {"m": "nobless_05", "n": ".....", "p": "/91/63/s_2726391.gif"},
  {"m": "jum0127", "n": ".....", "p": "N"},
  {"m": "agnes0317", "n": ".....", "p": "N"},
  {"m": "knato", "n": ".....", "p": "/27/10/s_1131027.gif"},
  {"m": "babiss", "n": ".....", "p": "N"},
  {"m": "pridekk", "n": ".....", "p": "N"},
  {"m": "cbk4660", "n": ".....", "p": "N"},
  {"m": "tokngwh", "n": "Crypto", "p": "N"}
]}

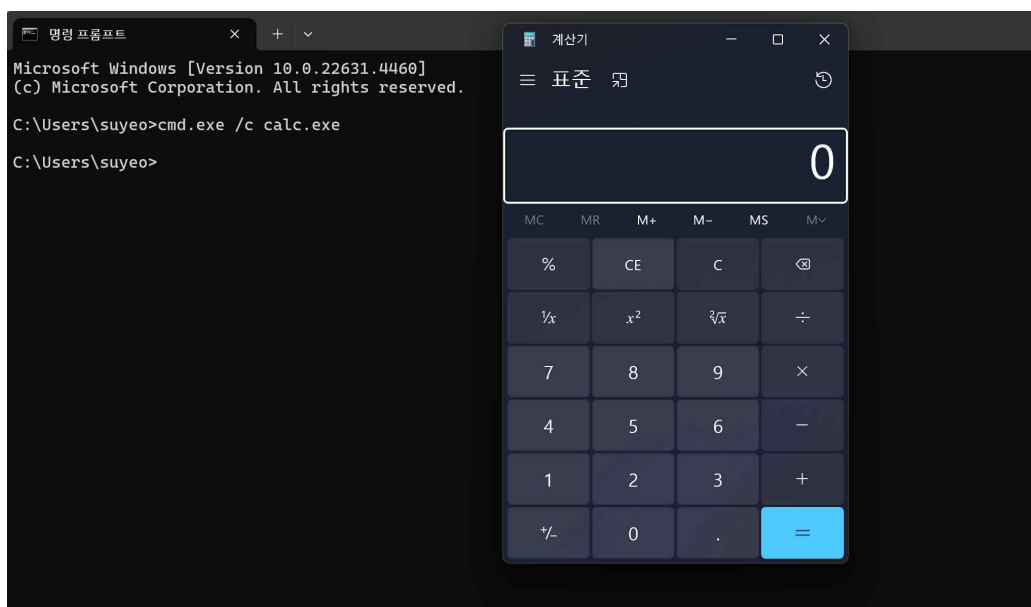
```

요청이 정상적으로 처리되었고, 응답 본문에 데이터가 포함
 서버는 Apache 웹 서버(버전 2.2.11)를 사용, mod_jk 모듈을 사용 중
 mod_jk는 Apache와 Tomcat 서버 간 통신을 지원하는 모듈
 P3P는 개인정보 보호 정책을 간략히 표현
 close: 응답 후 연결을 종료
 Content-Type: 응답 본문은 UTF-8 인코딩된 텍스트 데이터

```

Main.class
public class Main {
    public static void main(String[] args) throws Exception {
11      Runtime.getRuntime().exec("cmd.exe /c calc.exe");
    }
}

```



시스템 명령을 직접 실행하면 취약점이 노출될 수 있다.: 사용자 입력이 명령에 통합되면 명령 주입 공격이 발생할 수 있다. 악의적인 명령을 실행하면 시스템이 손상되거나 데이터 손상 가능성이 있다.

또한, 현재 코드는 악의적인 행위를 수행하지 않지만, 악성코드로 사용될 가능성이 높다.

특히, "JAR 파일 실행 -> 사용자 시스템에서 명령 실행"이라는 구조는 악성코드의 흔한 패턴이다. 안전한 환경에서 실행하고, 배포 방식이나 실행 목적에 주의해야함. 신뢰할 수 없는 환경에서 이 파일을 실행했다면 추가 보안 점검(예: 시스템 백도어 확인)을 권장한다.

```
OPTIONS / HTTP/1.1
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: lock.cmpxchg8b.com
Content-Length: 0
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 21 Jul 2010 02:34:12 GMT
Server: Apache
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

PROPFIND /calc.jar HTTP/1.1
Depth: 0
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/5.1.2600
Host: lock.cmpxchg8b.com
Content-Length: 0
Connection: Keep-Alive

HTTP/1.1 207 Multi-Status
Date: Wed, 21 Jul 2010 02:34:12 GMT
Server: Apache
Content-Length: 898
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/xml; charset="utf-8"
```

HTTP 메서드: OPTIONS

User-Agent: Windows XP 환경에서 실행된 WebDAV 클라이언트로 추정

200 OK: 요청이 정상적으로 처리

서버는 클라이언트와의 연결을 최대 5초 동안 유지하고, 최대 100개의 요청을 처리 가능

HTTP 메서드: PROPFIND

/calc.jar의 메타데이터를 요청

Depth: 0 : 현재 리소스에 대한 정보만 요청

207 Multi-Status: WebDAV의 응답 코드로, 여러 리소스 또는 속성의 상태를 포함


```
GET / HTTP/1.1
Accept: */*
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/1419897C-14C4645E2C2-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: www.google.co.kr
Connection: Keep-Alive
Cookie: PREF=ID=f740ee6473e4d08c:U=8b2018b6f27902d0:NW=1:TM=1279679410:LM=1279679411:S=VkJXrkGtNptuI1B5; NID=37=c0W9nJrlekq2l_qo
pgdasnrJd91lNEiJkrmuEX-mH9UJ_rBcDMpS_IDOX3AGAIHfcujNyPswM4c4dd-0ymzd5pu30tDtG4w7Y80dabjgH2ij3u8vhguwHRBGLdnQuze

HTTP/1.1 200 OK
Date: Wed, 21 Jul 2010 02:33:22 GMT
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Encoding: gzip
Server: igfe
Content-Length: 12150
X-XSS-Protection: 1; mode=block
```

Google 홈페이지의 기본 HTML을 요청

200 OK (정상 처리)

Content-Encoding: 응답 데이터가 GZIP으로 압축

Content-Type: HTML 문서임을 알 수 있음

Cookie - PREF 쿠키: 사용자의 기본 설정을 저장, NID 쿠키: Google 계정 인증 또는 사용자 추적에 사용

```
GET /ig/f/qXu29BUALEY/intl/ALL_kr/homepage_v3.css HTTP/1.1
Accept: */*
Referer: http://www.google.co.kr/
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 29 Jun 2010 21:50:07 GMT
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IPMS/1419897C-14C4645E2C2-000000030786; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2)
Host: www.google.co.kr
Connection: Keep-Alive
Cookie: PREF=ID=f740ee6473e4d08c:U=8b2018b6f27902d0:NW=1:TM=1279679410:LM=1279679411:S=VkJXrkGtNptuI1B5; NID=37=c0W9nJrlekq2l_qo
pgdasnrJd91lNEiJkrmuEX-mH9UJ_rBcDMpS_IDOX3AGAIHfcujNyPswM4c4dd-0ymzd5pu30tDtG4w7Y80dabjgH2ij3u8vhguwHRBGLdnQuze

HTTP/1.1 304 Not Modified
Date: Wed, 21 Jul 2010 02:33:22 GMT
Expires: Wed, 21 Jul 2010 01:04:42 GMT
Age: 0
Server: GFE/2.0
```

CSS 요청:

브라우저는 캐시된 CSS 파일을 비교하기 위해 If-Modified-Since 헤더를 포함.

서버는 파일이 수정되지 않았음을 응답(304 Not Modified).



고급검색언어도구

Google 검색 I'm Feeling Lucky

New! 구글 한국어 음성검색을 시험해 보세요

이 시간 인기 도록

[나경원 강용석 시건](#)
[백일섭 고두심 홍도아](#)
[조광래 축구 스타일은](#)
[허정무 감독 무릎팍 출연](#)
[한재이 로한 감독 수감](#)
[여중생 성매매 60대 지상](#)
[허정무 감독 말아먹었다](#)
[지나 폐지중계 창 삼아](#)
[노사연 美 원정출산 고백](#)
[아직은 집값 안정 우선](#)

인기 블로그

[\[정치\] 심학봉 강용석 여성의원 '몸뚱' 꺼지](#)
4시간 전 - 미디어토씨
한나라당이 성희롱 발언 파문을 일으킨 강용석 의원을 제명하거
로 결정했습니다. 당위 위신을 훼손했다는 이유입니다. 제명 정
[전체 블로그 127개 >](#)

화제의 인물



크롬 - 빠른 인터넷 브라우저

서비스 전체보기

패킷 흐름

1. Google 접속

- 클라이언트는 google.co.kr에 접속하기 위해 DNS 질의를 수행
- Google 서버(66.249.89.104)와 TCP 연결을 설정한 후, HTTP 요청을 통해 Google 홈페이지 데이터를 정상적으로 수신.
- 추가적으로 Google의 CSS 리소스와 성능 데이터를 요청(generate_204, csi)하며, 이는 google 서비스 사용 중 발생하는 일반적인 로깅과 성능 데이터 수집 패턴.

2. Naver 카페로 이동

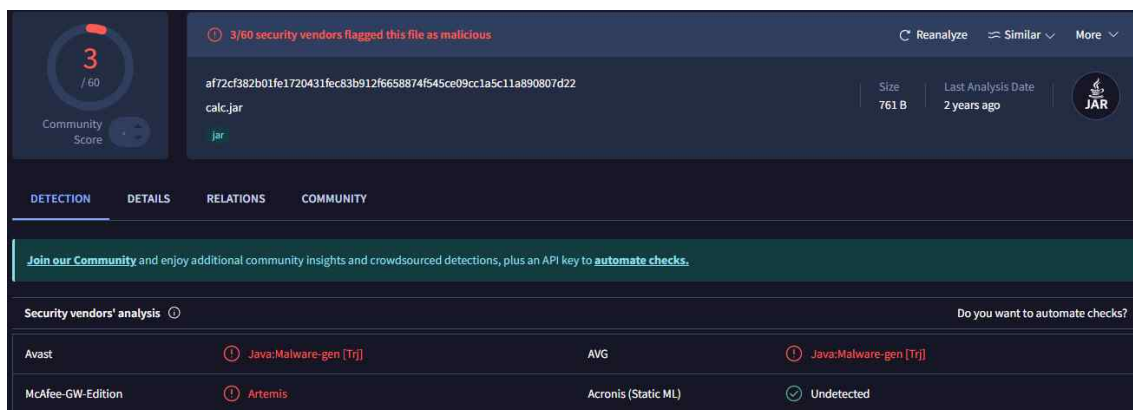
- Google에서 특정 링크를 통해 네이버 카페의 특정 게시글로 이동 (<http://cafe.naver.com>)
- 카페 게시글에서 외부 서버로 연결되는 링크를 발견.

3. 외부 서버 요청 및 JAR 파일 다운로드

- 네이버 카페의 특정 게시글(articleid=251)에서 외부 서버(lock.cmpxchg8b.com)로 연결.
- 클라이언트는 외부 서버에서 /calc.jar 파일을 요청
- 서버는 200 ok 응답과 함께 JAR 파일을 전달하며, MIME 타입은 application/x-java-archive로 설정

4. JAR 파일 다운로드

- 다운로드된 calc.jar 파일의 크기는 761바이트로 매우 작음.
- 서버 정보:
 - Apache 웹 서버 (2.2.11)
 - mod_jk 모듈을 통해 Apache와 Tomcat 간 통신 지원.
- 파일 메타데이터:
 - Lash-Modified 헤더를 통해 마지막 수정 날짜 제공.



The image shows a VirusShare analysis page for a file named 'calc.jar'. The file's SHA-256 hash is 'af72cf382b01fe1720431fec83b912f6658874f545ce09cc1a5c11a890807d22'. The file size is 761 B and it was last analyzed 2 years ago. A 'Community Score' of 3/60 is displayed. The 'DETECTION' tab is active, showing security vendors' analysis. Avast and McAfee-GW-Edition are listed as 'Undetected', while Artemis is marked as 'Java:Malware-gen [Trj]'. The AVG vendor is also listed as 'Java:Malware-gen [Trj]'. A banner at the top states '3/60 security vendors flagged this file as malicious'.

Security vendors' analysis	Do you want to automate checks?
Avast	Java:Malware-gen [Trj]
McAfee-GW-Edition	Artemis
Acronis (Static ML)	Undetected

실행 시 cm d.exe를 호출하여 calc.exe를 실행

시스템에서 calc.exe파일이 존재하거나 악성 파일로 추가 다운로드될 가능성이 있음.

바이러스 토탈 분석했을 때 Avast: Java:Malware-gen [Trj], McAfee: Artemis 검출

Avast: Java:Malware-gen [Trj]

이름의 의미:

Java: 악성코드가 Java 기반 파일(예: JAR, CLASS)에서 발견되었음을 나타냄.

Malware-gen: Generic Malware의 약자로, 알려진 악성코드와 유사한 동작 패턴을 가진 일반적인 악성코드임을 의미.

[Trj]: Trojan(트로이 목마)으로 분류되는 악성코드임을 나타냄.

특징:

Avast는 Malware-gen으로 탐지된 악성코드가 의심스러운 동작을 포함하고 있음을 의미합니다. 예를 들어:

시스템 명령 실행(cmd.exe 호출).

파일 다운로드 및 실행.

네트워크 연결을 통해 추가적인 악성코드 유포.

정확한 악성코드의 종류를 특정하지는 못했지만, 일반적으로 악성 패턴을 기반으로 탐지.

McAfee: Artemis

이름의 의미:

Artemis는 McAfee에서 사용하는 고급 위협 탐지 시스템의 코드명입니다.

클라우드 기반 분석을 통해 알려지지 않은 잠재적 악성코드를 탐지할 때 주로 사용됩니다.

특징:

McAfee는 Artemis라는 이름을 통해 파일이 의심스럽거나 악성 코드로 간주된다고 경고합니다.

이 탐지는 악성코드의 특정 서명(Signature)이나 동작 기반 분석(Behavioral Analysis)에 의해 이루어짐.

보통 네트워크 트래픽, 실행 동작, 코드 구조 등을 클라우드 서버에서 실시간으로 비교하여 탐지.