

# **1. Okay-bommer (2019-11-12)**

<https://www.malware-traffic-analysis.net/2019/11/12/index.html>

## 1-1. 구성 환경

### 구성 환경

---

LAN segment range: 10.11.11.0/24 (10.11.11.0 through 10.11.11.255)

Domain: okay-boomer.info

Domain controller: 10.11.11.11 - Okay-Boomer-DC

LAN segment gateway: 10.11.11.1

LAN segment broadcast address: 10.11.11.255

### TIP

---

1. 사이트에 접속한 운영체제나 디바이스 타입을 알고 싶을 때 Wireshark 필터

`http.request and ip.addr eq x.x.x.x`

2. IP주소의 Mac address을 알고 싶을 때 Wireshark 필터

`ip.src eq x.x.x.x`

3. 사이트에 접속한 Host name, Account name을 알고 싶을 때 wireshark 필터

`kerberos.CnameString and ip.addr eq x.x.x.x`

4. 파일 추출 및 SHA 파일 출력

파일 추출 : 패킷 오른쪽 클릭 -> Follow -> TCP Stream

SHA 파일 출력 : `shasum -a 256 filename`

5. 악성코드분석 사이트

<https://www.virustotal.com>

70 개의 악성코드 분석 엔진의 해쉬값 비교를 통해 악성 여부를 판단하여 결과를 보여줌

Malware.com 결과와 함께 비교해서 판단하면 좀 더 정확하게 악성 여부에 대한 판단이 가능

## 1-2. 문제 및 해답

### 문제 및 해답

Q. What operating system and type of device is on 10.11.11.94?

: ChromeOS on a Chromebook

Q. What operating system and type of device is on 10.11.11.121?

: Samsung Galaxy Note 8

Q. What operating system and type of device is on 10.11.11.179?

: macOS 10.15.1 (Catalina) on a Mac (desktop or Macbook)

Q. What version of Windows is being used on the host at 10.11.11.195?

: Windows 10

Q. What operating system and type of device is on 10.11.11.217?

: iPadOS 13.2.2 on an iPad

The image displays two screenshots from the Wireshark network protocol analyzer. The top screenshot shows a packet list with a filter 'http.request and ip.addr eq 10.11.11.94' applied. A packet from 10.11.11.94 to 10.11.11.217 is selected, and a context menu is open with 'Follow' and 'TCP Stream' options. The bottom screenshot shows the 'Follow TCP Stream' view for the selected packet, displaying an HTTP GET request to chromebooktrivia.com. The User-Agent string is 'Mozilla/5.0 (X11; CrOS x86\_64 12239.92.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36'. Annotations include an arrow pointing to the 'CrOS' part of the User-Agent and text stating 'CrOS stands for: ChromeOS' and 'ChromeOS is used on Chromebooks'.

**CrOS** stands for: ChromeOS

ChromeOS is used on Chromebooks

```
GET / HTTP/1.1
Host: chromebooktrivia.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; CrOS x86_64 12239.92.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/76.0.3809.136 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 303 See Other
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
```



Q. Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?

: Motorola

2019-11-12-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src eq 10.11.11.145

Time	Src	port	Dst	port	Info
2019-11-11 22:22:01	10.11.11.145	3...	8.8.8.8	53	Standard
2019-11-11 22:22:20	10.11.11.145	4...	173.194.67.188	5228	Applicati
2019-11-11 22:22:20	10.11.11.145	4...	173.194.67.188	5228	41835 → 5
2019-11-11 22:22:31	10.11.11.145	3...	127.0.0.1	53	Standard
2019-11-11 22:23:00	10.11.11.145	3...	8.8.8.8	53	Standard

Frame 20560: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

Ethernet II, Src: Motorola bc:2d:98 (bc:ff:eb:bc:2d:98), Dst: Cisco\_97:4b:f0

Internet Protocol Version 4, Src: 10.11.11.145, Dst: 8.8.8.8

User Datagram Protocol, Src Port: 33656, Dst Port: 53

Domain Name System (query)

**MAC address shows vendor as "Motorola"**

Q. What is the user account name used to log into the Windows host at 10.11.11.200?

: brandon.gilbert

Q. What is the host name and Windows user account name used on that IP address?

: host name - Tucker-Win7-PC, user account name - candice.tucker

kerberos.CNameString and ip.addr eq 10.11.11.203

Time	Src	port	Dst	port	Info
2019-11-11 22:21:13	10.11.11.11	88	10.11.11.203	49164	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49166	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49168	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49173	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49174	TGS-REP
2019-11-11 22:21:22	10.11.11.203	49179	10.11.11.11	88	AS-REQ
2019-11-11 22:21:22	10.11.11.203	49180	10.11.11.11	88	AS-REQ
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49180	AS-REP
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49181	TGS-REP
2019-11-11 22:21:47	10.11.11.203	49182	10.11.11.11	88	AS-REQ
2019-11-11 22:21:47	10.11.11.203	49183	10.11.11.11	88	AS-REQ
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49183	AS-REP
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49184	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49186	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49188	TGS-REP
2019-11-11 22:21:48	10.11.11.11	88	10.11.11.203	49191	TGS-REP
2019-11-11 22:21:49	10.11.11.11	88	10.11.11.203	49192	TGS-REP
2019-11-11 22:22:12	10.11.11.11	88	10.11.11.203	49194	TGS-REP
2019-11-11 22:22:12	10.11.11.11	88	10.11.11.203	49195	TGS-REP
2019-11-11 22:36:32	10.11.11.11	88	10.11.11.203	49223	TGS-REP

CNameString

TUCKER-WIN7-PC\$

kerberos.CNameString and ip.addr eq 10.11.11.203

Time	Src	port	Dst	port	CNameString	Info
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49166	TUCKER-WIN7-PC\$	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49168	TUCKER-WIN7-PC\$	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49173	TUCKER-WIN7-PC\$	TGS-REP
2019-11-11 22:21:14	10.11.11.11	88	10.11.11.203	49174	TUCKER-WIN7-PC\$	TGS-REP
2019-11-11 22:21:22	10.11.11.203	49179	10.11.11.11	88	TUCKER-WIN7-PC\$	AS-REQ
2019-11-11 22:21:22	10.11.11.203	49180	10.11.11.11	88	TUCKER-WIN7-PC\$	AS-REQ
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49180	TUCKER-WIN7-PC\$	AS-REP
2019-11-11 22:21:22	10.11.11.11	88	10.11.11.203	49181	TUCKER-WIN7-PC\$	TGS-REP
2019-11-11 22:21:47	10.11.11.203	49182	10.11.11.11	88	candice.tucker	AS-REQ
2019-11-11 22:21:47	10.11.11.203	49183	10.11.11.11	88	candice.tucker	AS-REQ
2019-11-11 22:21:47	10.11.11.11	88	10.11.11.203	49183	candice.tucker	AS-REP

Q. What IP is a Windows host that downloaded a Windows executable file over HTTP?

: 10.11.11.203

Q. What is the URL that returned the Windows executable file?

: http://acjabogados.com/40group.tiff

Q. What is the SHA256 file hash for that Windows executable file?

: 8d5d36c8ffb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635

Q. What is the detection rate for that SHA256 hash on VirusTotal?

: 49 of 70

The image shows a Wireshark packet capture analysis of an HTTP GET request. The top section displays the packet list and packet details. The packet list shows a packet from 188.95.248.71 to 10.11.11.203 on port 80. The packet details show the HTTP request for /40group.tiff. The packet bytes pane shows the raw data of the request, including the 'MZ' magic number for an executable file.

**ip contains "This program"**

**Destination IP is 10.11.11.203**

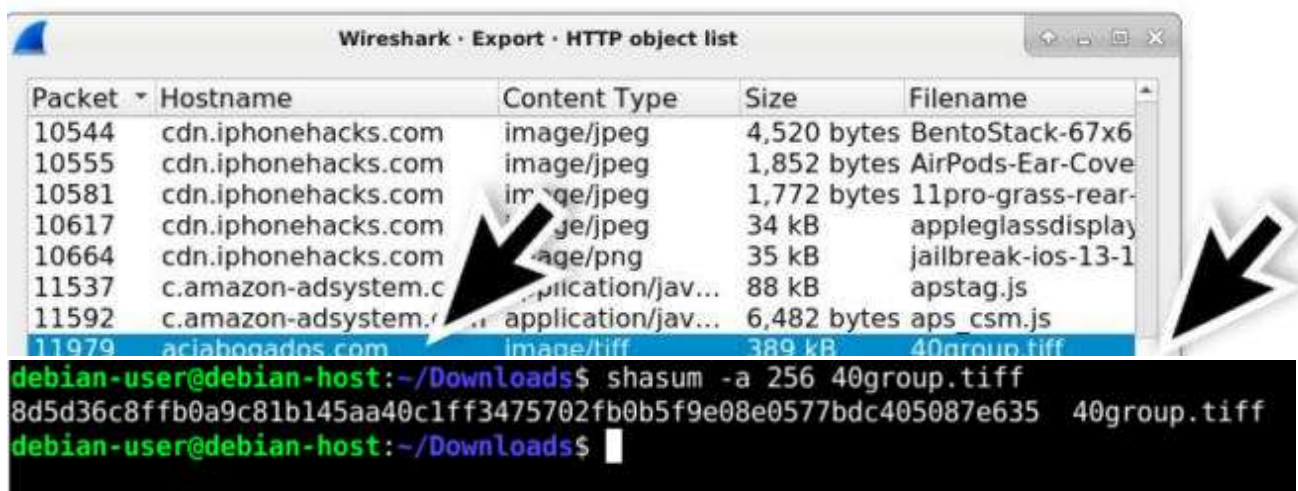
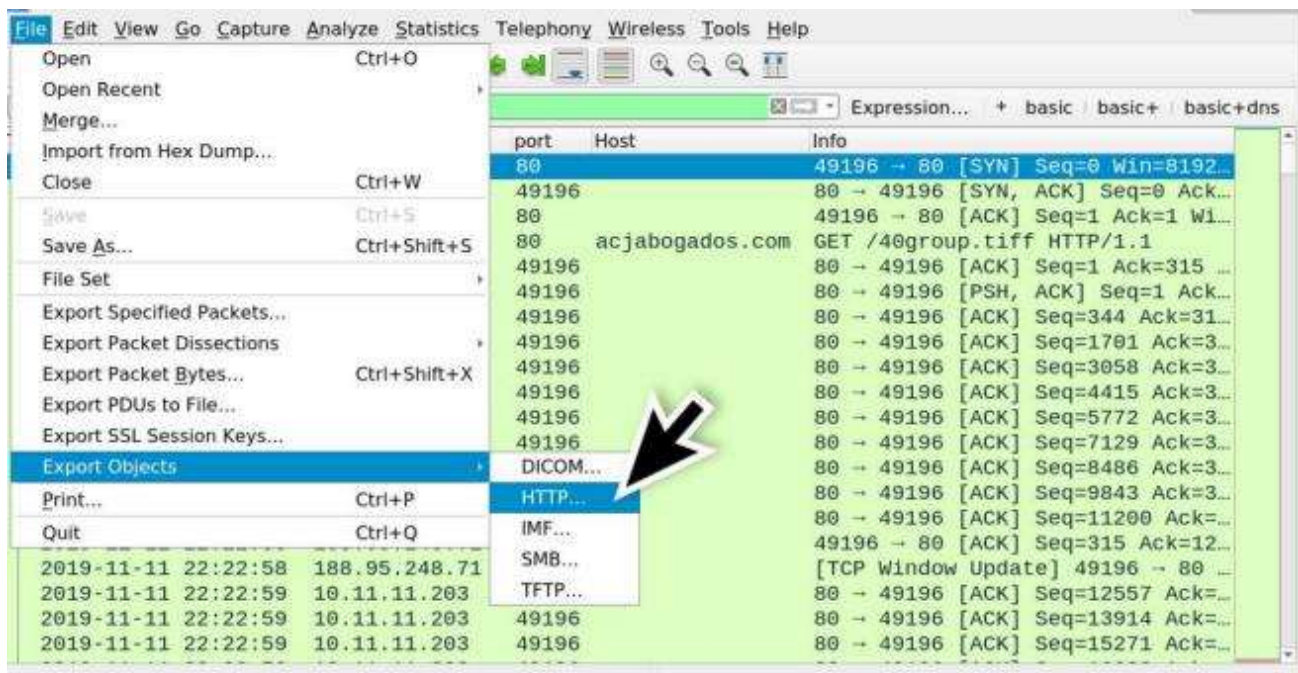
**http://acjabogados.com/40group.tiff**

**First two bytes of an EXE or DLL file show as "MZ"**

**This type of line commonly found in EXE or DLL files**

**This program cannot be run in DOS mode.**

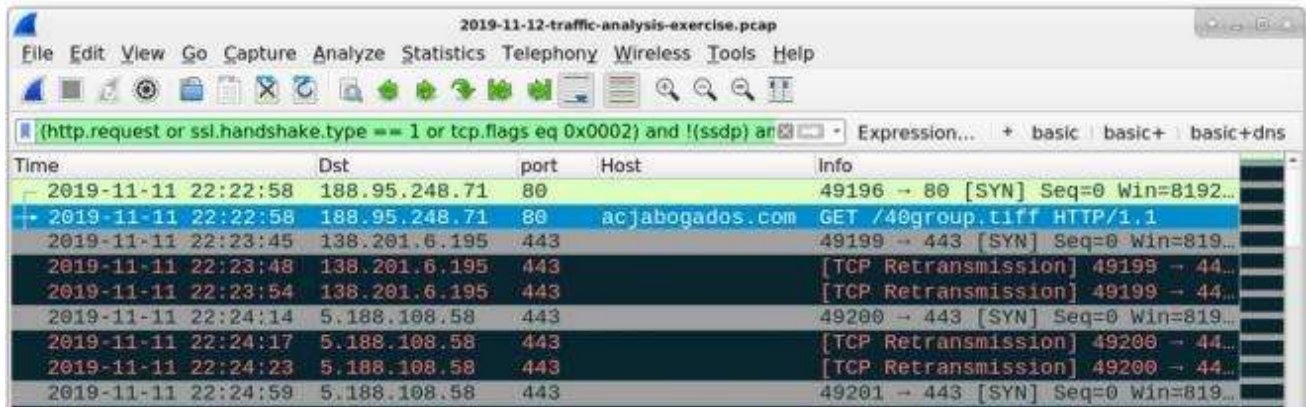




Q. What public IP addresses did that Windows host attempt to connect over TCP after the executable file was downloaded?

: 5.188.108.58 and 138.201.6.195

**and ip.addr eq 10.11.11.203 and !(ip.dst eq 10.11.11.11)**



Time	Dst	port	Host	Info
2019-11-11 22:22:58	188.95.248.71	80		49196 → 80 [SYN] Seq=0 Win=8192...
2019-11-11 22:22:58	188.95.248.71	80	acjabogados.com	GET /40group.tiff HTTP/1.1
2019-11-11 22:23:45	138.201.6.195	443		49199 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:23:48	138.201.6.195	443		[TCP Retransmission] 49199 → 44...
2019-11-11 22:23:54	138.201.6.195	443		[TCP Retransmission] 49199 → 44...
2019-11-11 22:24:14	5.188.108.58	443		49200 → 443 [SYN] Seq=0 Win=819...
2019-11-11 22:24:17	5.188.108.58	443		[TCP Retransmission] 49200 → 44...
2019-11-11 22:24:23	5.188.108.58	443		[TCP Retransmission] 49200 → 44...
2019-11-11 22:24:59	5.188.108.58	443		49201 → 443 [SYN] Seq=0 Win=819...