

# **Malware Traffic Analysis with Wireshark**

## **2016-12-17 - Your Holiday Present**

<https://malware-traffic-analysis.net./2016/12/17/index.html>

IS 401/501

9/11/2023

Group Members:

Patrick Doolin, Casen Woody, Isaac Vaillancourt, Josh Catterall,

Isaac Falero, Aaron Thammavongsa



### 3. IP address of the infected Windows computer.

2016-12-17-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Packet details Narrow & Wide Case sensitive String 00:1c:23:9b:70:5e

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	2016-12-16 20:30:38.380781	0.000000	172.16.2.254	172.16.2.96	DHCP	342	DHCP Offer - T
2	2016-12-16 20:30:38.381631	0.000850	172.16.2.254	172.16.2.96	DHCP	342	DHCP ACK - T
3	2016-12-16 20:30:38.407902	0.026271	172.16.2.96	224.0.0.22	IGMPv3	60	Membership Report
4	2016-12-16 20:30:38.415673	0.007771	172.16.2.96	224.0.0.22	IGMPv3	60	Membership Report
5	2016-12-16 20:30:38.417565	0.001892	172.16.2.96	224.0.0.252	LLMNR	69	Standard query 0x
6	2016-12-16 20:30:38.473073	0.055508	172.16.2.96	172.16.2.1	NBNS	110	Registration NB F
7	2016-12-16 20:30:38.473308	0.000235	172.16.2.96	172.16.2.1	NBNS	110	Registration NB F

```

> Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: Cisco_ba:37:f1 (00:09:b6:ba:37:f1), Dst: Dell_9b:70:5e (00:1c:23:9b:70:5e)
  > Destination: Dell_9b:70:5e (00:1c:23:9b:70:5e)
  > Source: Cisco_ba:37:f1 (00:09:b6:ba:37:f1)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.16.2.254, Dst: 172.16.2.96
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (Offer)

```

**Answer:** 172.16.2.96

**Explanation:** Search, using the find feature, for the MAC address found in part 2. This will show the IP of the infected Windows computer based off the destination of the first packet.

### 4. Host name of the infected Windows computer.

2016-12-17-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

nbns

No.	Time	Delta	Source	Destination	Protocol	Length	Info
6	2016-12-16 20:30:38.473073	0.055508	172.16.2.96	172.16.2.1	NBNS	110	Registration NB FROGGY-PC<20>
7	2016-12-16 20:30:38.473308	0.000235	172.16.2.96	172.16.2.1	NBNS	110	Registration NB FROGGY-PC<00>
8	2016-12-16 20:30:38.473967	0.000659	172.16.2.96	172.16.2.1	NBNS	110	Registration NB WORKGROUP<00>

```

> Ethernet II, Src: Dell_9b:70:5e (00:1c:23:9b:70:5e), Dst: Cisco_ba:37:f1 (00:09:b6:ba:37:f1)
> Internet Protocol Version 4, Src: 172.16.2.96, Dst: 172.16.2.1
> User Datagram Protocol, Src Port: 137, Dst Port: 137
v NetBIOS Name Service
  Transaction ID: 0xabbb2
  > Flags: 0x2900, Opcode: Registration, Recursion desired
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  > Queries
v Additional records
  v FROGGY-PC<20>: type NB, class IN
    Name: FROGGY-PC<20> (Server service)
    Type: NB (32)
    Class: IN (1)
    Time to live: 3 days, 11 hours, 20 minutes
    Data length: 6
  > Name flags: 0x6000, ONT: Unknown (H-node, unique)
    Addr: 172.16.2.96

```

**Answer:** FROGGY-PC

**Explanation:** Filter for “nbns”. This will reveal all of the NBNS traffic. You can then correlate the MAC and IP address found in part 2 and 3 to identify the host name of the infected Windows computer.

## 5. The person's name (or account name) using the infected Windows host.

2016-12-17-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

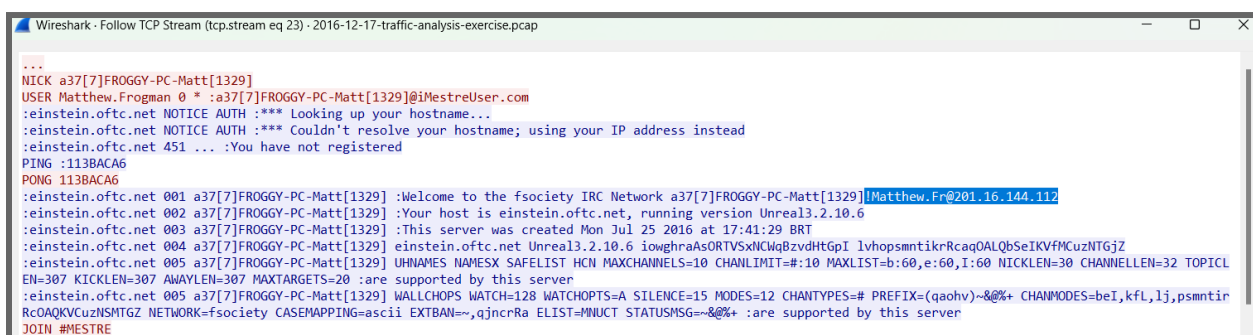
http.request

No.	Time	Source	Destination	Protocol
73	11.205616	172.16.2.96	187.33.238.74	HTTP
117	121.103032	172.16.2.96	65.181.125.20	HTTP
199	125.349529	172.16.2.96	74.117.178.179	HTTP



**Explanation:** Adding host as a column and filtering by http.request we see several GETs within the TCP stream that have malware like /bibi/aw7.tff, /bibi/dll.exe

## 7. Public IP address of the infected Windows computer.



```

...
NICK a37[7]FROGGY-PC-Matt[1329]
USER Matthew.Frogman 0 * :a37[7]FROGGY-PC-Matt[1329]@iMestreUser.com
:einstein.oftc.net NOTICE AUTH :*** Looking up your hostname...
:einstein.oftc.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:einstein.oftc.net 451 ... :You have not registered
PING :113BAC6
PONG 113BAC6
:einstein.oftc.net 001 a37[7]FROGGY-PC-Matt[1329] :Welcome to the fsociety IRC Network a37[7]FROGGY-PC-Matt[1329]||Matthew.Fr@201.16.144.112
:einstein.oftc.net 002 a37[7]FROGGY-PC-Matt[1329] :Your host is einstein.oftc.net, running version Unreal3.2.10.6
:einstein.oftc.net 003 a37[7]FROGGY-PC-Matt[1329] :This server was created Mon Jul 25 2016 at 17:41:29 BRT
:einstein.oftc.net 004 a37[7]FROGGY-PC-Matt[1329] :einstein.oftc.net Unreal3.2.10.6 iowghraAsORTVSxNCWqBzvdHtGpI lyhopsmtikrRcaq0ALQbSeIKVfMCuzNTGjZ
:einstein.oftc.net 005 a37[7]FROGGY-PC-Matt[1329] :UHNames NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICL
EN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported by this server
:einstein.oftc.net 005 a37[7]FROGGY-PC-Matt[1329] :WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaoHV)~&@%+ CHANMODES=beI,kfL,lj,psmntir
RcOaQKVCuzNSMTGZ NETWORK=fsociety CASEMAPPING=ascii EXTBAN=~,qjncrRa ELIST=MNUCT STATUSMSG=~&@%+ :are supported by this server
JOIN #MESTRE

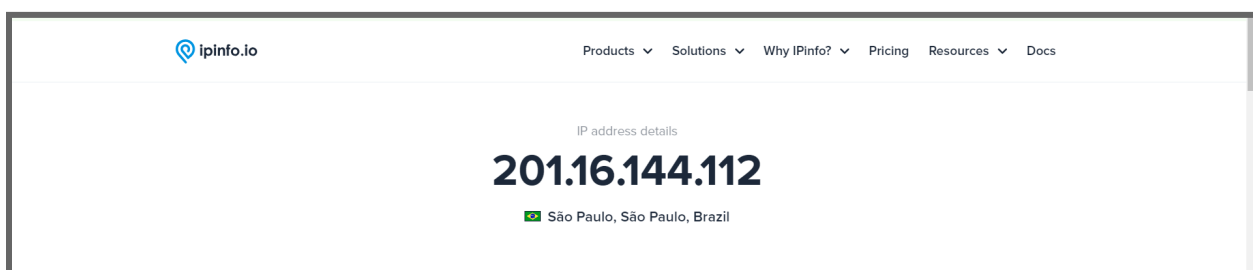
```

**Answer:** 201.16.144.112

**Evidence:** Matthew Frogman first appears in packet 484 with the destination IP of 65.181.112.240 and a host of www.devyatinsky.ru.

**Explanation:** Filter by IP addresses using the IP address found in the packet. Use the filter ip.addr eq 65.181.112.240 then follow the traffic by following the TCP stream. Matthew Frogman's public IP address is found here.

## 8. The country or general location of the infected Windows computer.



**Answer:** Brazil

**Evidence:** ipinfo.io shows that Frogman's IP address is Brazilian.

### **Division of Labor**

All of the members collaborated to complete this lab. Prompts were divided and tackled according to the member's skills. Aaron Thammavongsa ran and projected virtualization software used to perform the lab. Documentation was completed by Isaac Vaillancourt, Patrick Doolin, and Casen Woody. Screenshots were taken and inserted by Josh Catterall and Isaac Falero.