

## #PCAP-ANALYSIS | Example-01

For each pcap, answer the following questions:

1. What is the date and time of the activity?
2. What is the IP address of the Windows host that gets infected?
3. What is the domain name and IP address of the compromised web site?
4. What is the domain name and IP address that delivered the exploit kit (EK)?
5. What is the name of the EK?

### File-01

1. What is the date and time of the activity?  
The pcap starts at 2015-01-08 23:51:21 UTC and ends at 23:52:04 UTC.
2. What is the IP address of the Windows host that gets infected?  
192.168.138.158
3. What is the domain name and IP address of the compromised web site?  
IP address: 108.168.211.93  
Domain: [www.subaruoutback.org](http://www.subaruoutback.org)
4. What is the domain name and IP address for the exploit kit?  
IP address: 205.234.186.112  
Domain: atypefresh.in
5. What is the name of the EK?  
Fiesta

### File-02

1. What is the date and time of the activity?  
The pcap starts at 2015-01-14 15:27:20 UTC and ends at 15:34:18 UTC.
2. What is the IP address of the Windows host that gets infected?  
192.168.204.137
3. What is the domain name and IP address of the compromised web site?  
IP address: 188.227.165.20  
Domain: freeforgames.com
4. What is the domain name and IP address for the exploit kit?  
IP address: 5.196.214.27  
Domain: 20.c368.464.75b43b.e3161.dec8.033da1.8c.hl39dj2plwle.lowamounts.in
5. What is the name of the EK?  
Magnitude

.pcap analysis automatically online:

<https://packettotal.com/app/analysis?id=9b1fd402bab9d97330804982a29cd83d>

NOTE: This pcap contains callback traffic for one of the malware payloads, a CryptoWall 3.0 sample that I blogged about in the SANS Internet Storm Center at: <https://isc.sans.edu/diary/Traffic+Patterns+For+CryptoWall+30/19203>