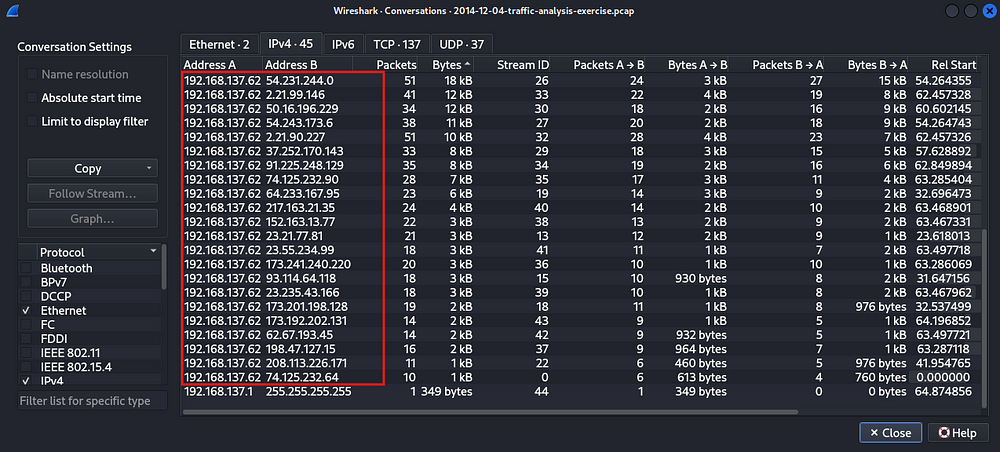
**Analysis of Malicious Network Traffic**

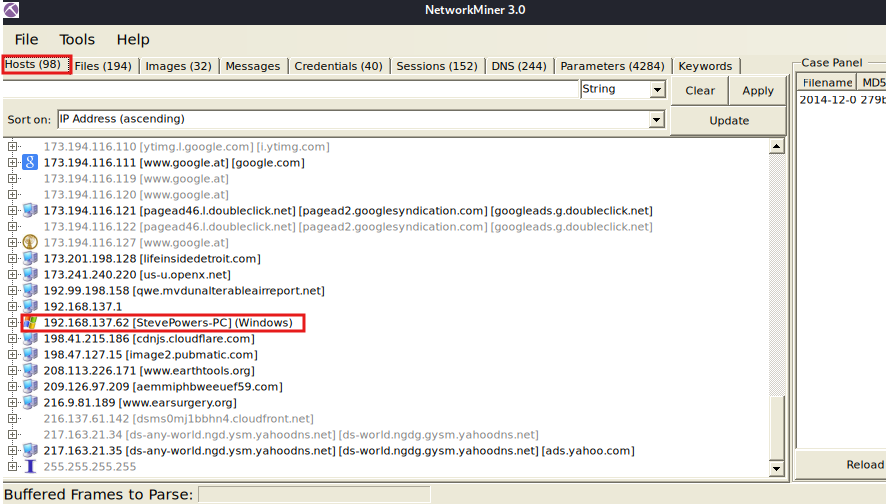
A network capture file containing traffic associated with an Exploit Kit attack has been provided. The purpose of this analysis is to determine the precise sequence of events culminating in the delivery of the Exploit Kit.

**1. Identify the IP address of the compromised Windows host.**

Examination of the conversation statistics will reveal the IP addresses involved in the highest volume of network traffic.



Analysis reveals that IP address 192.168.137.62 established the highest volume of connections. Further examination using Network Miner is recommended to ascertain the compromised host.

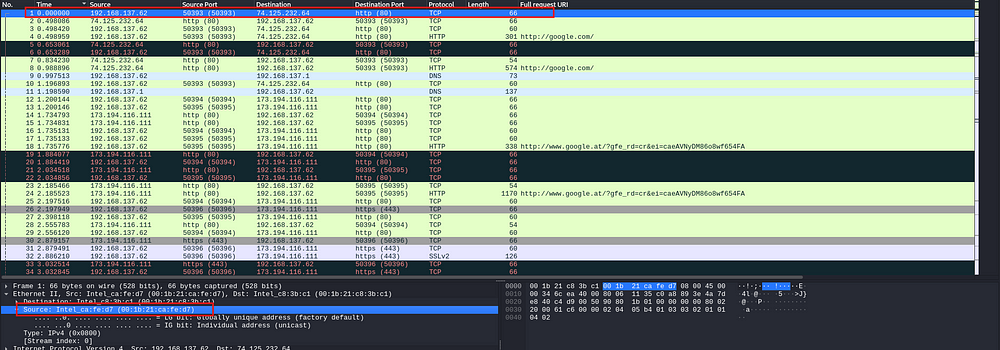


Examination of the network traffic using NetworkMiner reveals a single Windows host present within the captured data.

**Answer:** 192.168.137.62

**Question 2: What is the Media Access Control (MAC) address of the compromised Windows host?**

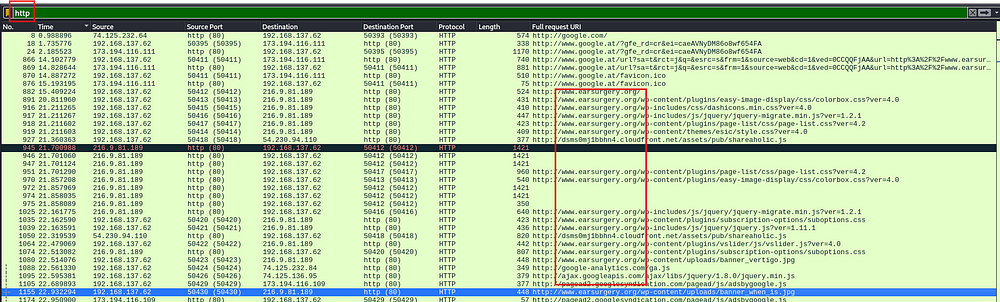
To ascertain the MAC address, a packet originating from IP address 192.168.137.62 will be selected, and its Ethernet frame will be analyzed.



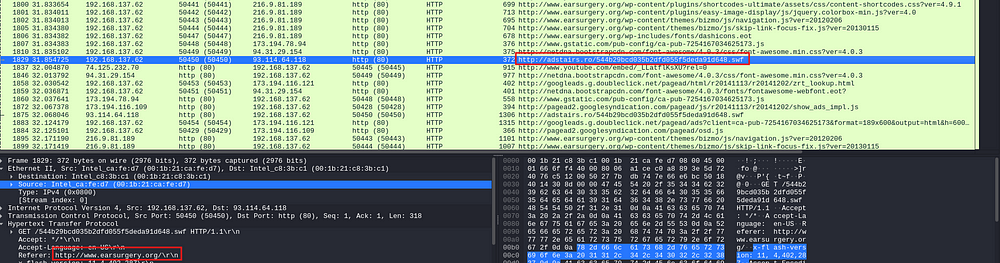
**Answer:** 00:1b:21:ca:fe:d7

**3. What is the domain name of the compromised web site?**

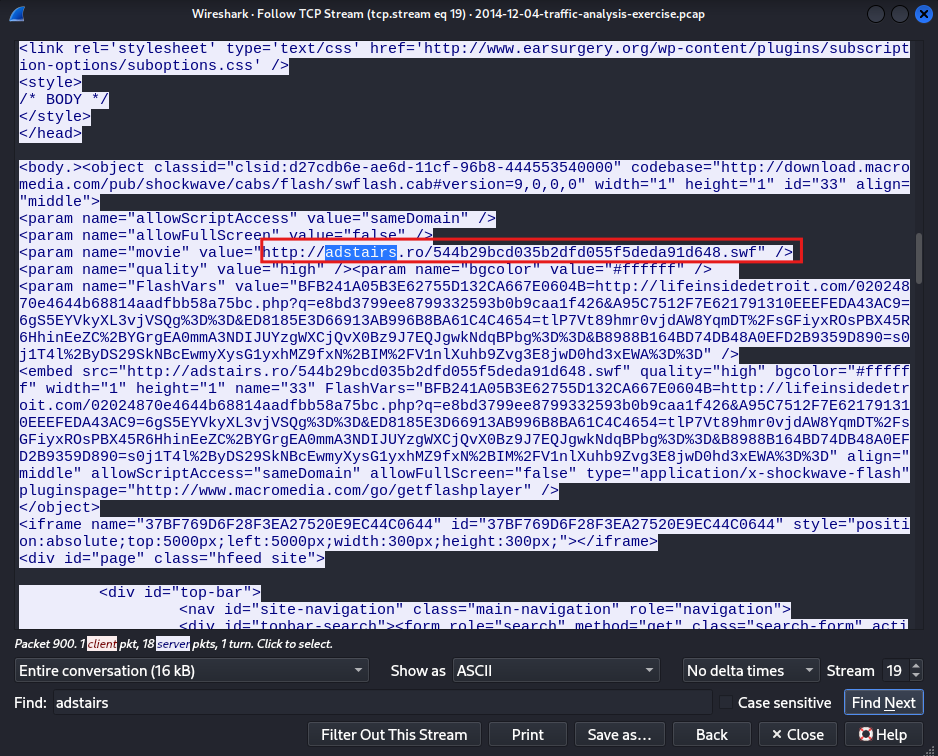
We shall examine HTTP requests by applying the filter "http".



Examination of network traffic reveals a significant volume of requests directed towards www.earsurgery.org. Further analysis of the HTTP traffic indicates a request originating from the earsurgery.org webpage to adstairs.ro/….swf.



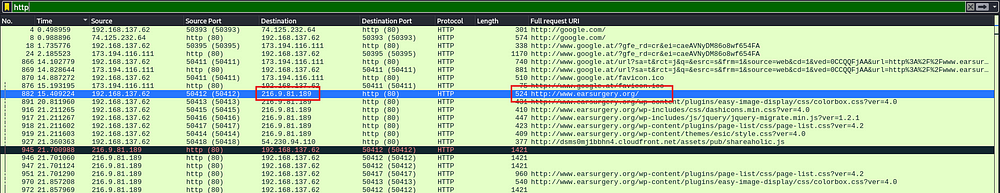
An examination of the source code for the "earsurgery" website will be conducted.



As evidenced above, the site adstairs is embedded within and concealed by the earsurgery website. Upon a user accessing and loading the earsurgery website, a subsequent request is initiated to the adstairs site.

Answer: www[.]earsurgery[.]org

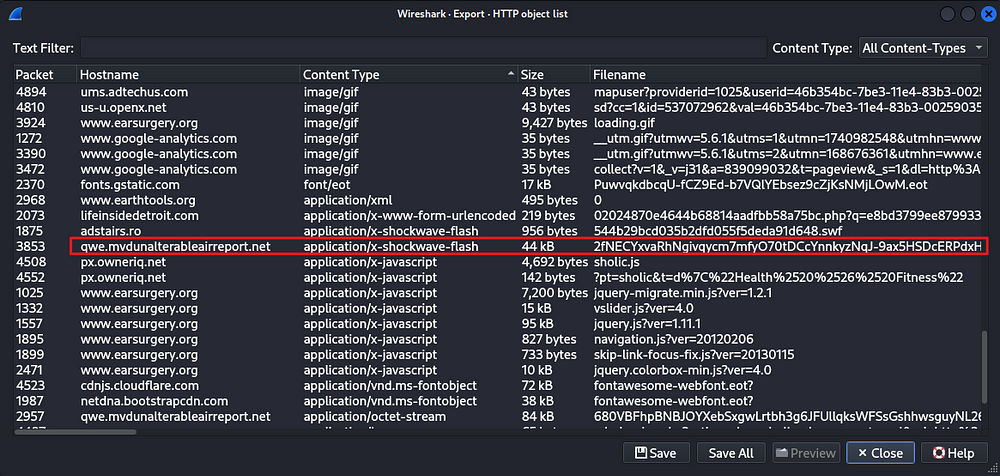
4. What is the IP address of the compromised web site?



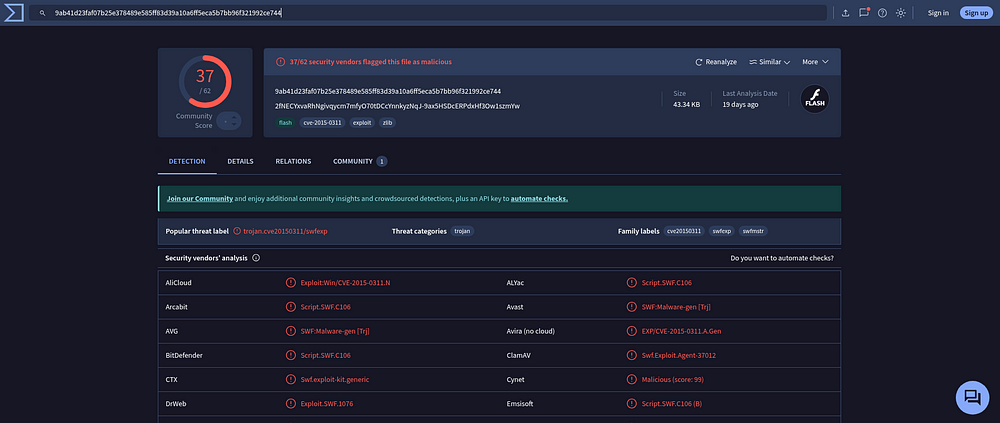
**Answer:** 216.9.81.189

**5. What is the domain name that delivered the exploit kit and malware payload?**

We shall now examine the HTTP objects to identify any malicious files..



Analysis of HTTP objects revealed a Flash file. Downloading and evaluating its reputation is recommended.



Consequently, the downloaded file is identified as malicious. The corresponding domain name is...

Answer: qwe[.]mvdunalterableairreport[.]net

**6. What is the IP address that delivered the exploit kit and malware payload?**

**Answer:** 192.99.198.158

**MORE ADVANCED QUESTIONS:**

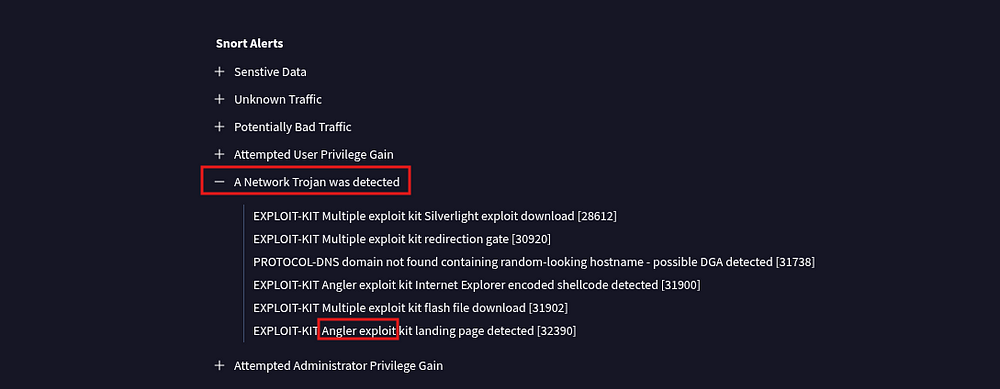
**7. What snort events (either VRT or EmergingThreats) are generated by this pcap?**

Upload the file to VirusTotal. Subsequently, navigate to the details pane and scroll to the end. The triggered Snort alerts will then be visible.



**8. What is the exploit kit (EK)?**

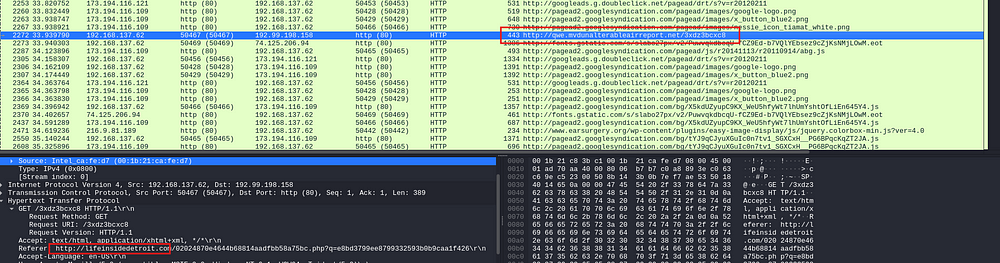
Within the Snort rules, navigate to the section labeled "A Network Trojan Was Detected." The exploit kit's identifier will be visible therein.



**Answer:** Angler exploit.

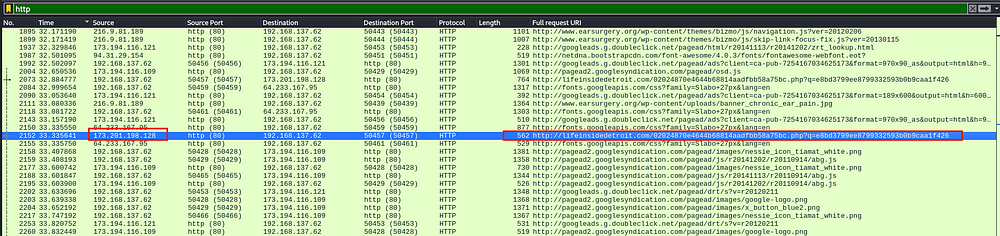
**9. What is the redirect URL that points to the exploit kit (EK) landing page?**

Return to the initial packet of the website's loading sequence to examine the HTTP header for referer details.



**Answer:** lifeinsidedetroit[.]com

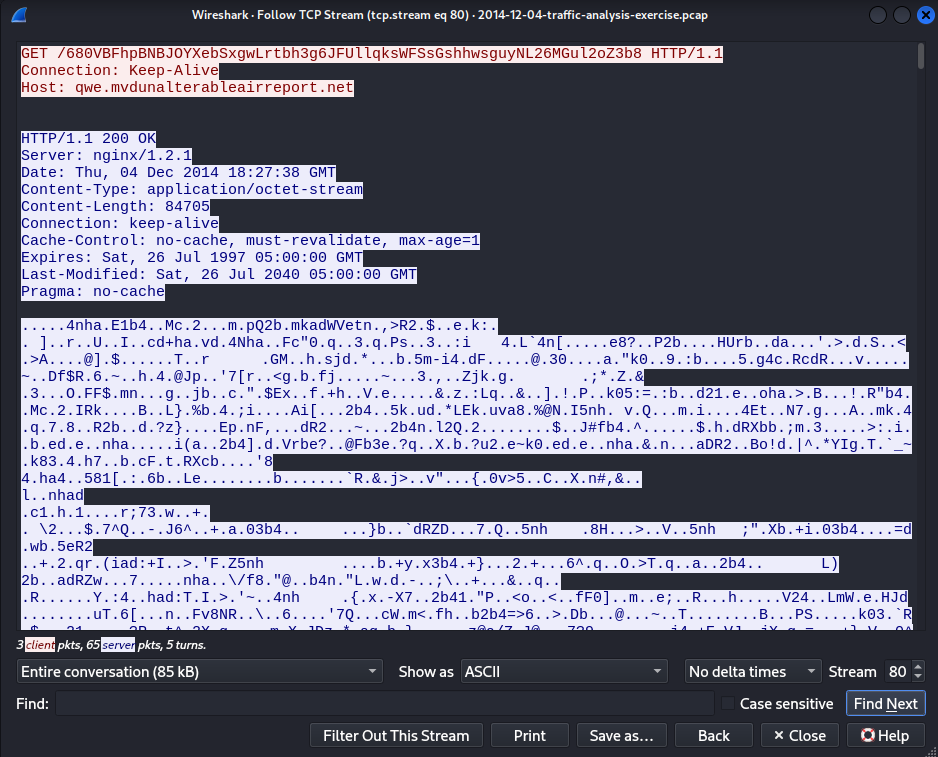
**10. What is the IP address of the redirect URL that points to the exploit kit (EK) landing page?**



**Answer:** 173.201.198.128

**11. Which tcp stream shows the malware payload being delivered?**

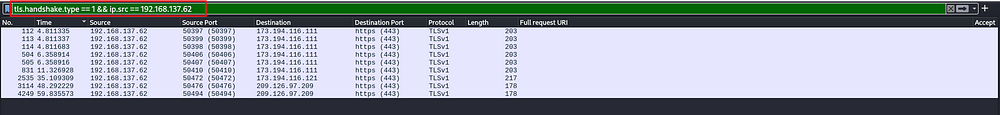
Transmission Control Protocol (TCP) stream 80 is responsible for delivering the malicious binary, which constitutes the final phase of the malware deployment process.



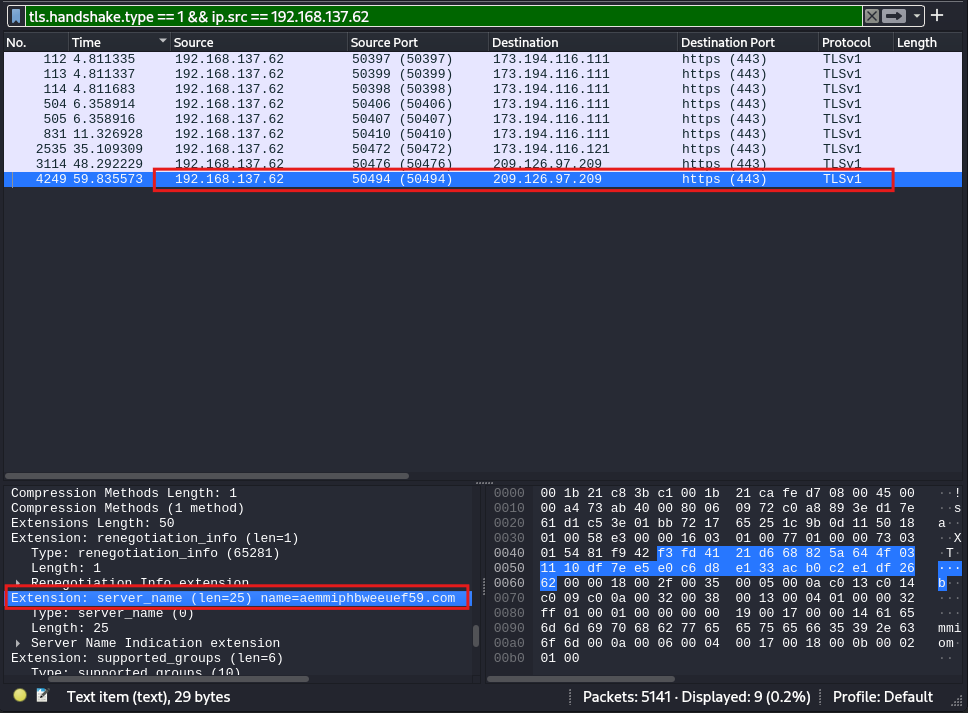
**Answer:** tcp stream eq 80

**12. What is the domain name and IP address of the HTTPS callback traffic caused by this malware infection?**

Let us examine the TLS handshake packets to determine if any HTTPS requests were initiated by the subject system.



We will proceed with the analysis of packet data to identify any anomalous network connections.



**Answer:** aemmiphbweeuef59[.]com 209[.]126[.]97[.]200