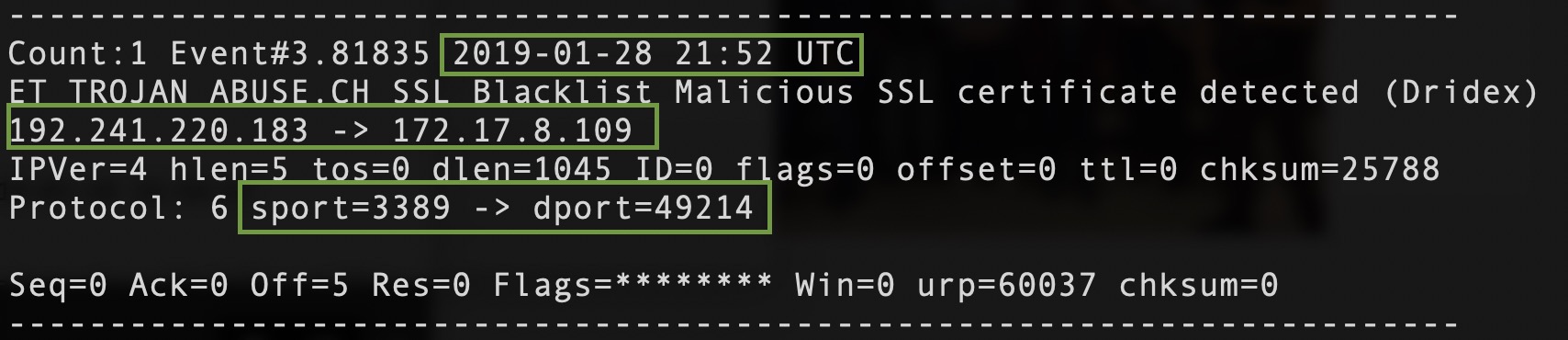
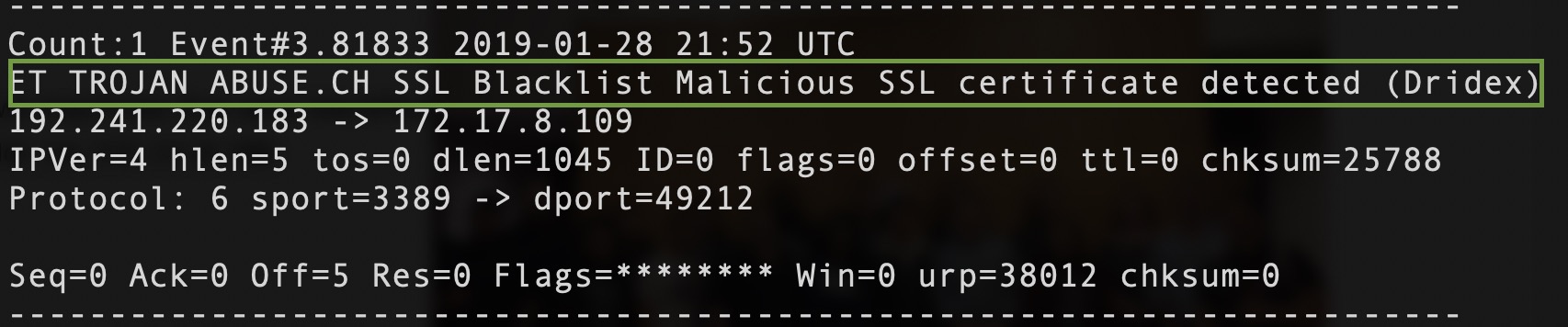
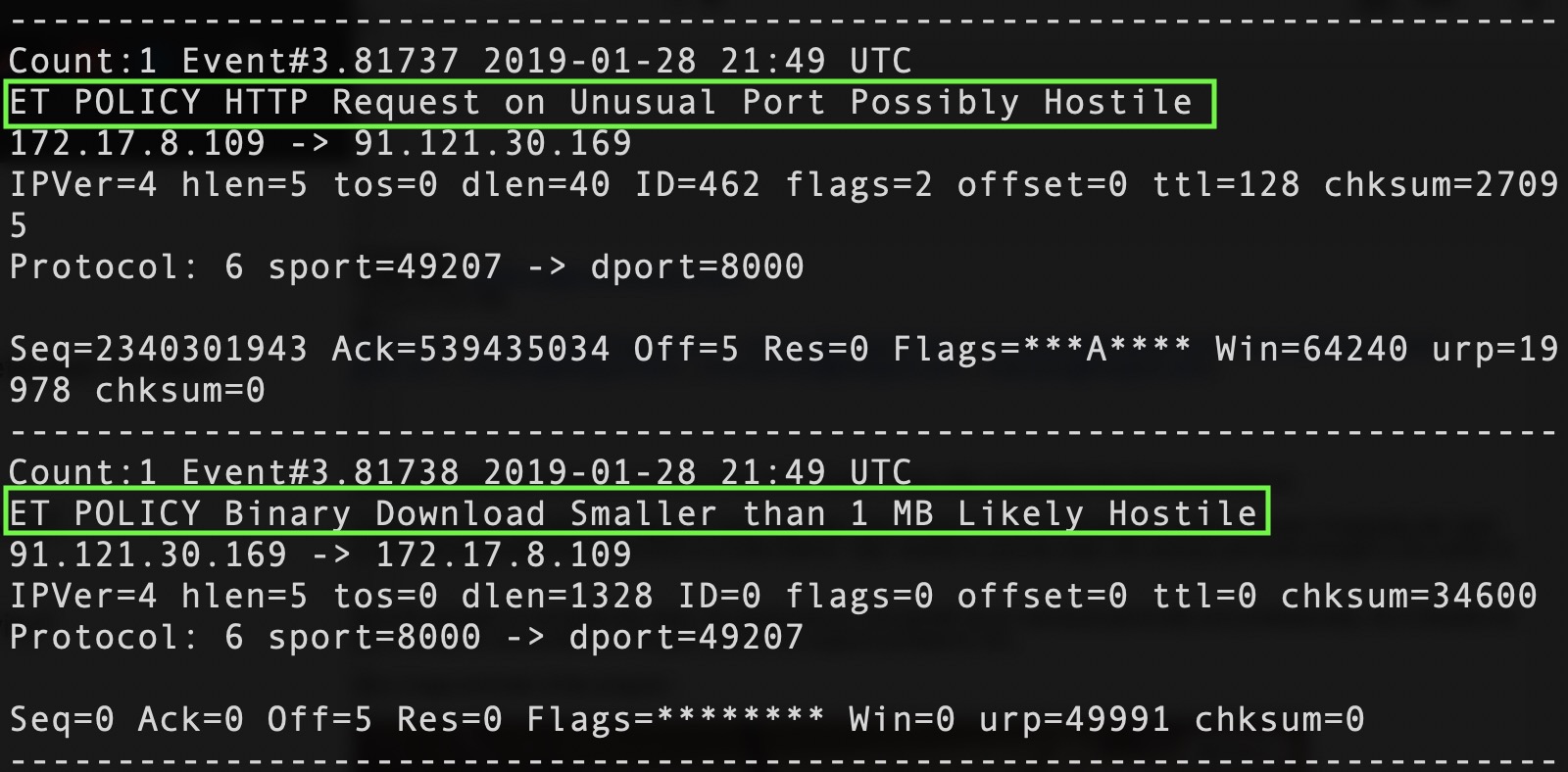
**POST INCIDENT REPORT**

What activity is snort reporting on?

* GET POLICY HTTP Request on Unusual Port Possibly Hostile
* GET POLICY Binary Download Smaller than 1 MB Likely Hostile
* GPL SHELLCODE x86 NOOP
* GET POLICY PE EXE or DLL Windows file download HTTP
* GET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
* GET TROJAN ABUSE.CH SSL Blacklist Malicious SSL Certificate Detected

What is the date and time of this alert?

* 2019-01-28 21:49 UTC

What is the external IP address that snort is flagging for malicious activity?

* 91.121.30.169

What is the internal IP address that snort is flagging for malicious activity?

* 172.17.8.109

What is the source port of the activity?

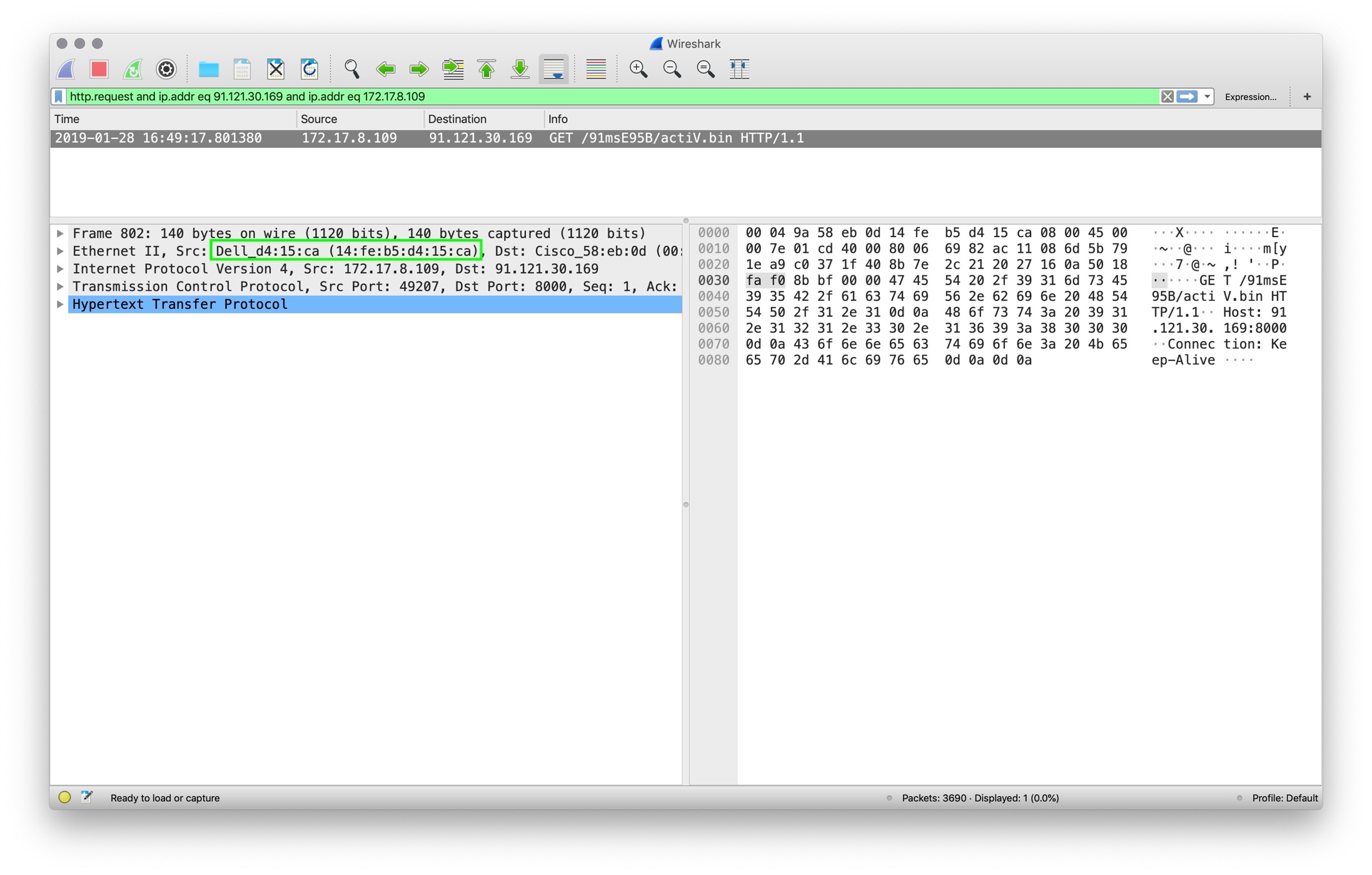
* 8000

What is the destination port of the activity?

* 49207

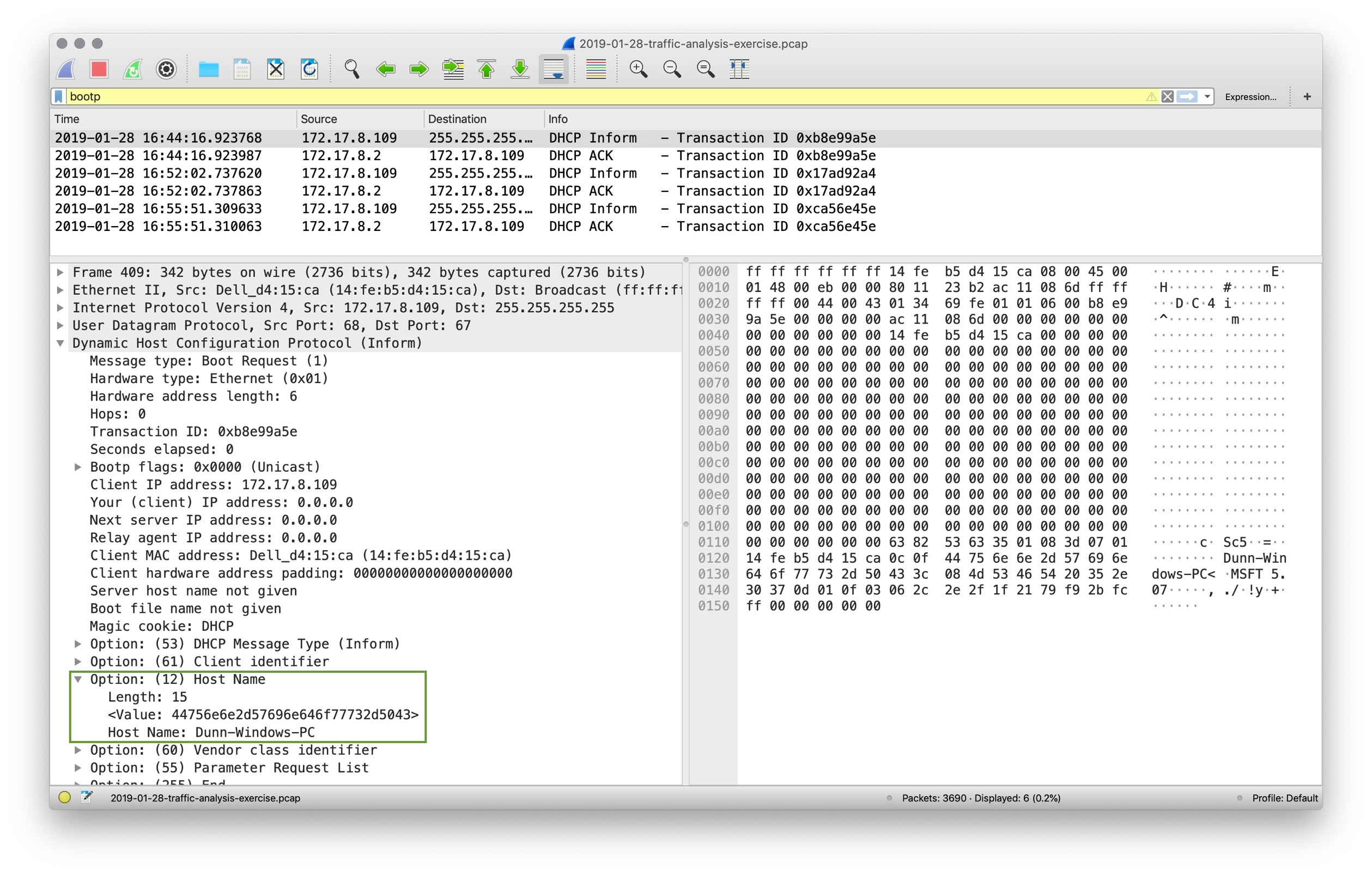
What is the MAC address of the internal computer involved?

* DELL (14:fe:b5:d4:15:ca)



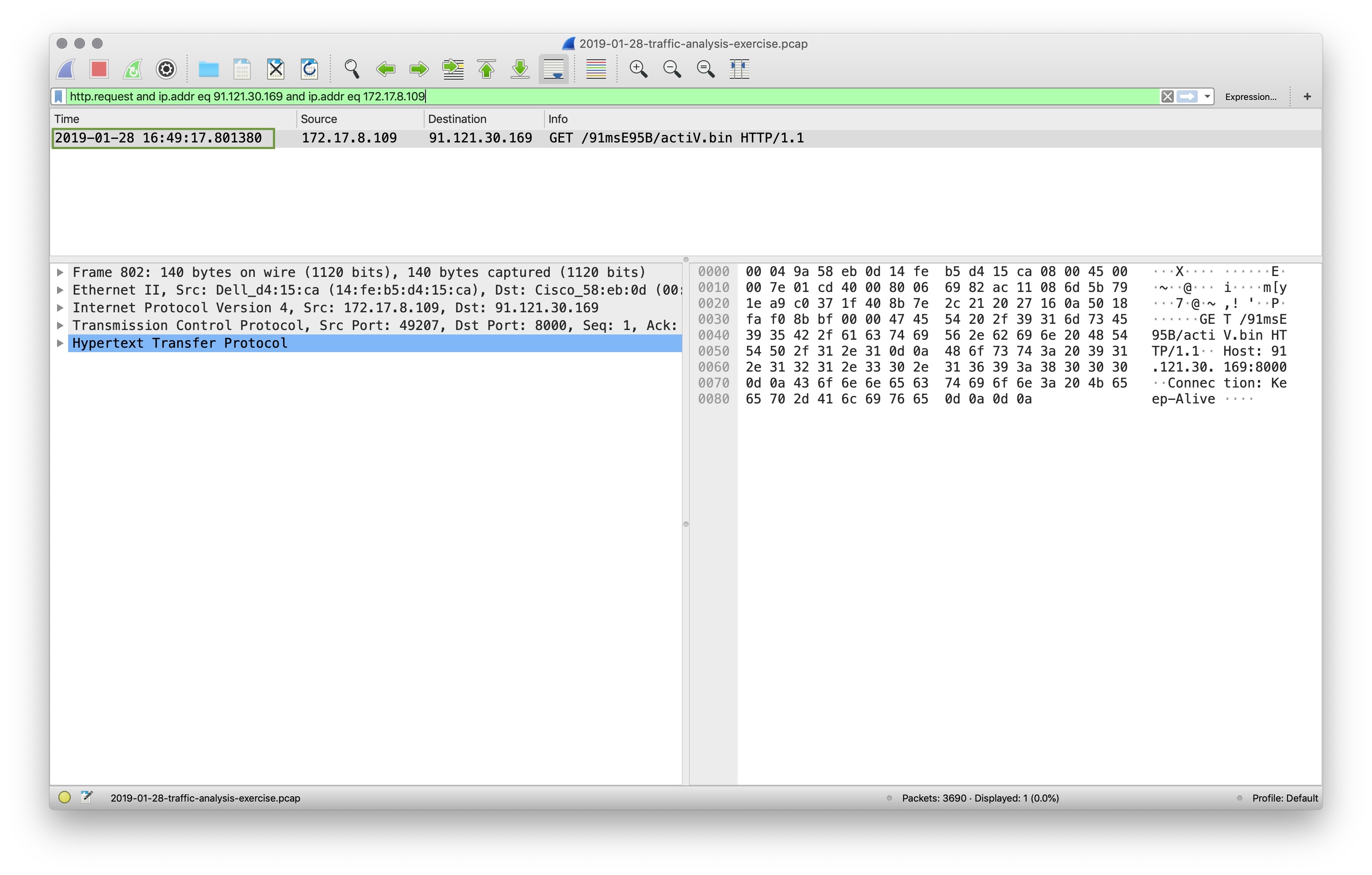
What is the host name of the internal machine?

* By filtering using ‘bootp’ you can see below the host name is ‘Dunn-Windows-PC’



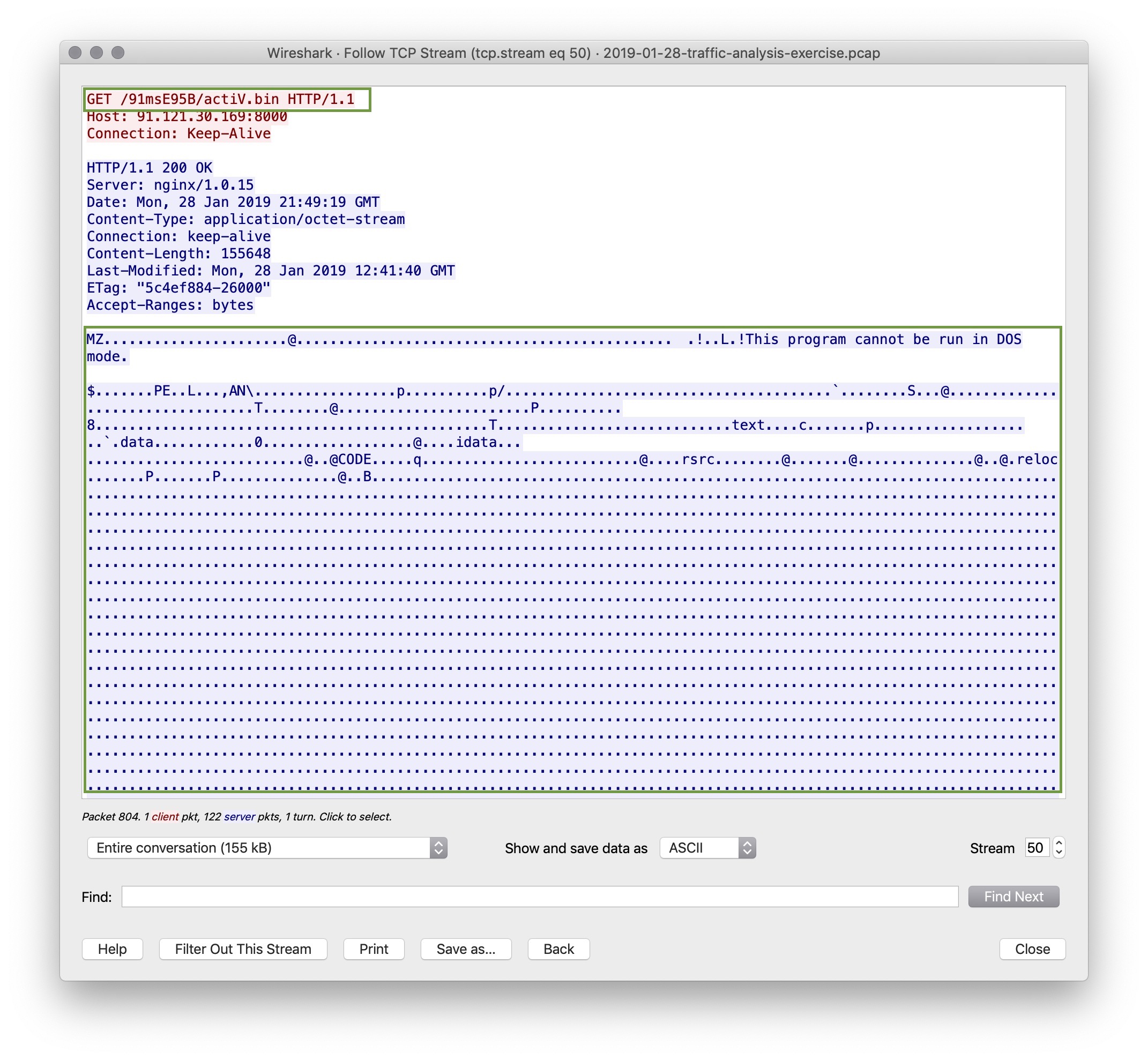
Can you confirm the date and time this issue occurred?

* Yes, it occurred 2019-01-28 16:49:17.801380



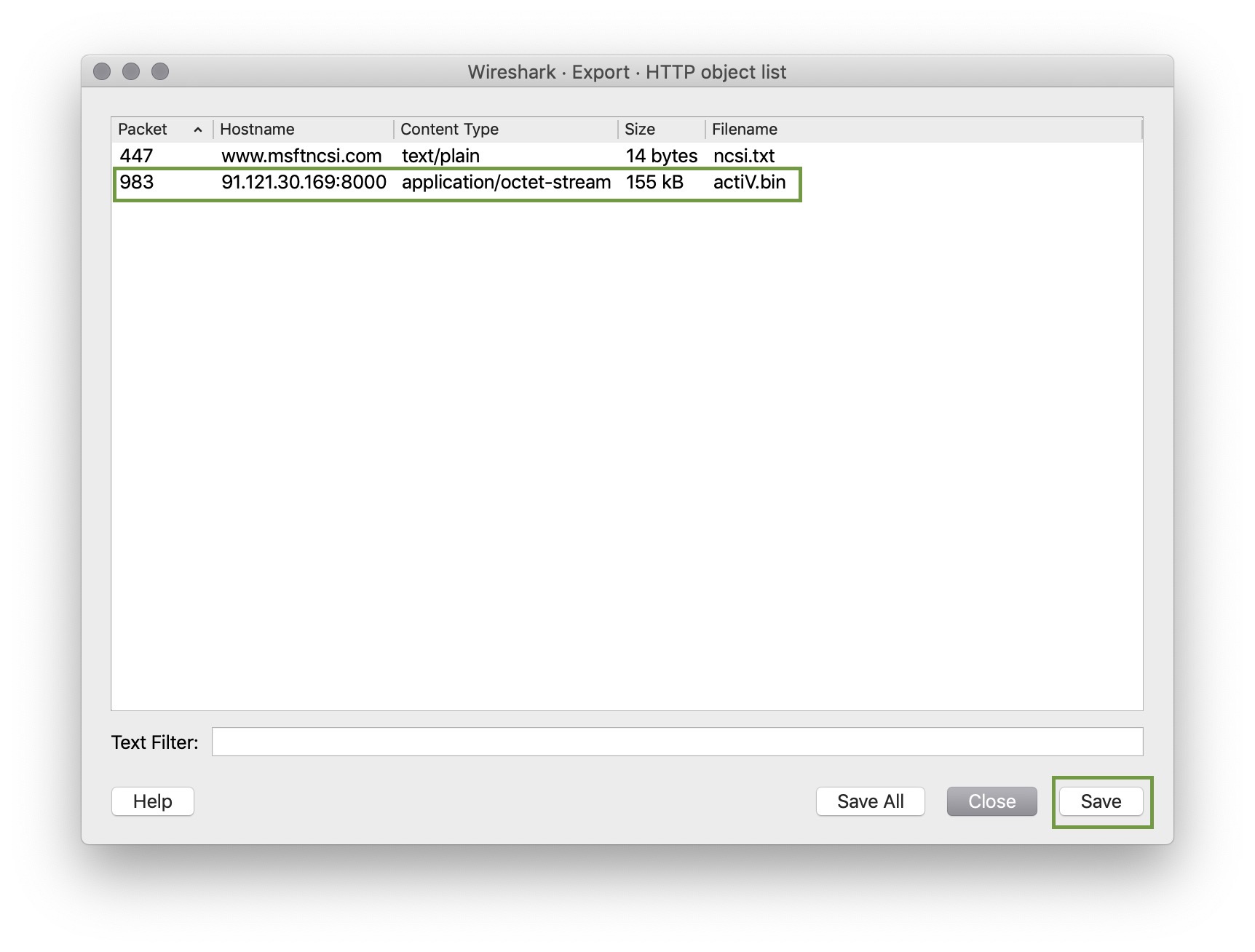
How can you confirm the if the snort alert is accurate?

* When the TCP stream is followed, you can see the binary download starting with ‘MZ’ and ‘!This program cannot be run in DOS mode.’ (See below)



Can you verify whether or not malware was downloaded?

* If you go to File > Export Objects > HTTP’
* You will see active.bin file which should be saved
* Once hashed in terminal using md5sum you can go to virustotal.com to verify if it is a true positive.



If this issue needs to be mitigated what steps should be taken with the infected machine?

* The machine should be restored from a prior known good backup or backup before infection took place.

What steps should be taken in regards to network security?

* Using wireshark you can set a rule for the offending ip address (91.121.30.169/32)
* Knowing this information you can blacklist the IP
* Another solution and more probable is to white list known good internal IP addresses.

Would you categorize this as a Web, Email, or Network attack?

* This attack was carried out by a victim clicking a malicious web link; therefore, this is a Web Attack.