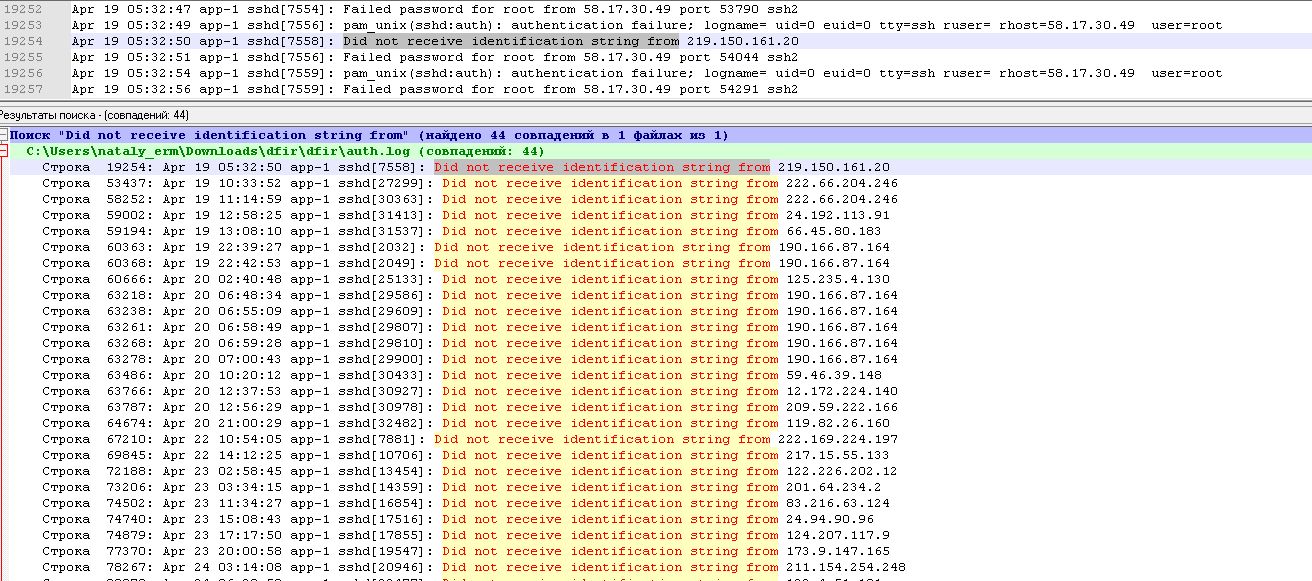
### **Forensics3**

Задача: Кажется, сайт взломали еще раз. Сможете найти опознавательный знак взломщика, которые проникли на сервер? Хорошо бы узнать его адрес.

Решение:

В приложенном архиве нам будет интересен файл auth.log, тк там есть все логи с каких ip были входы.

Файл можно открыть, например, в Notepade++ и вытащить все ip по слову “from” и проанализировать неудавшиеся попытки входа, например, по строкам “Did not receive identification string from”. Нашлось 44 строки:



Попробую под поле ответа внести первый ip - 219.150.161.20.

Удачно.