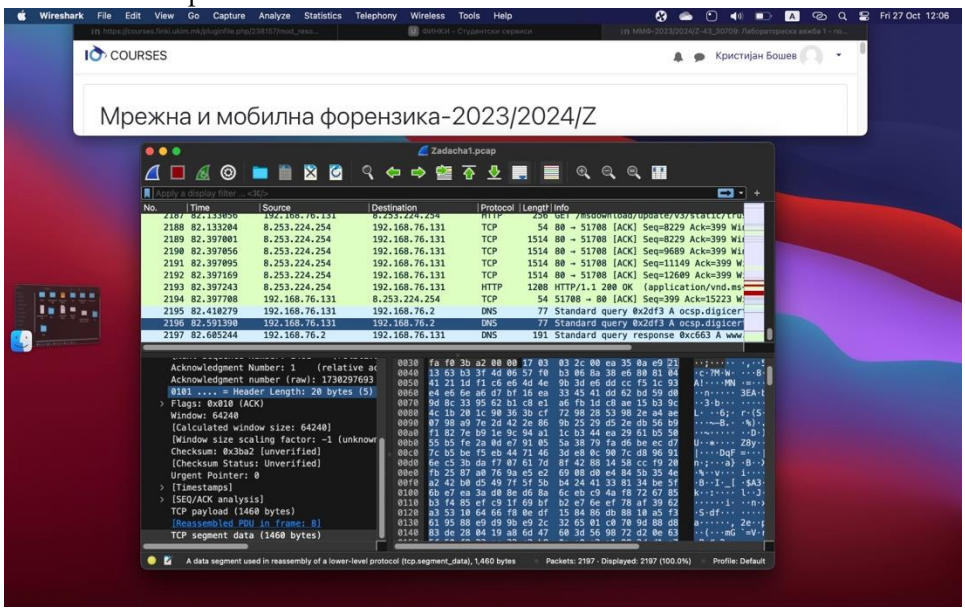
Лабораториска вежба 1 – Анализа на мрежен сообраќај и лог датотеки	*Име и презиме* *Кристијан Бошев*	*Индекс* *203159*

Напомена: Сите одговори треба да бидат напишани со црвена боја. На секој screenshot што ќе го поставите во елаборатот, осигурајте се дека се гледа вашето најавено име на Courses и моменталното време.

Дел 1

1. Колку вкупно пакети се фатени?



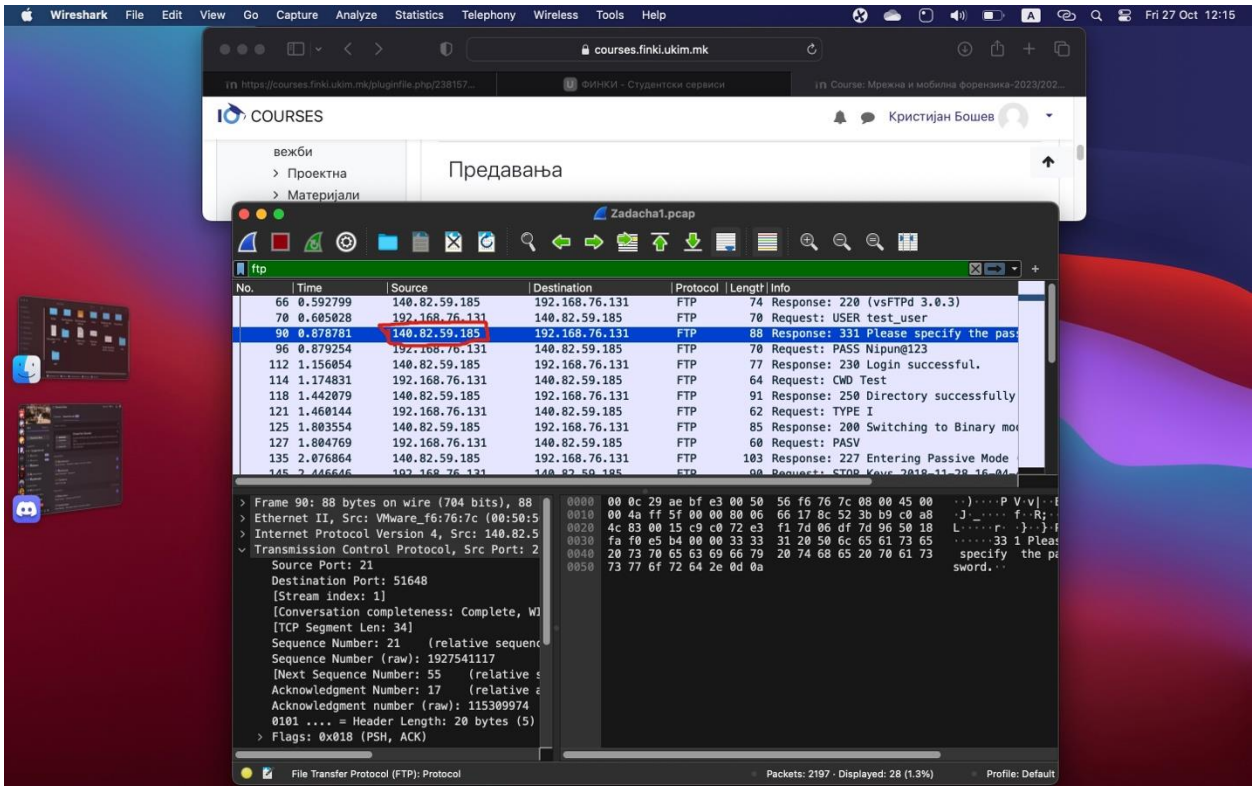
Одговор:

2. Дали некој од филтрите врати резултати? Кој? Што утврдивте и дали нешто изгледа сомнително?

   Одговор: Секој од филтрите врати одреден резултат, во зависност тоа што ни треба и кој протокол

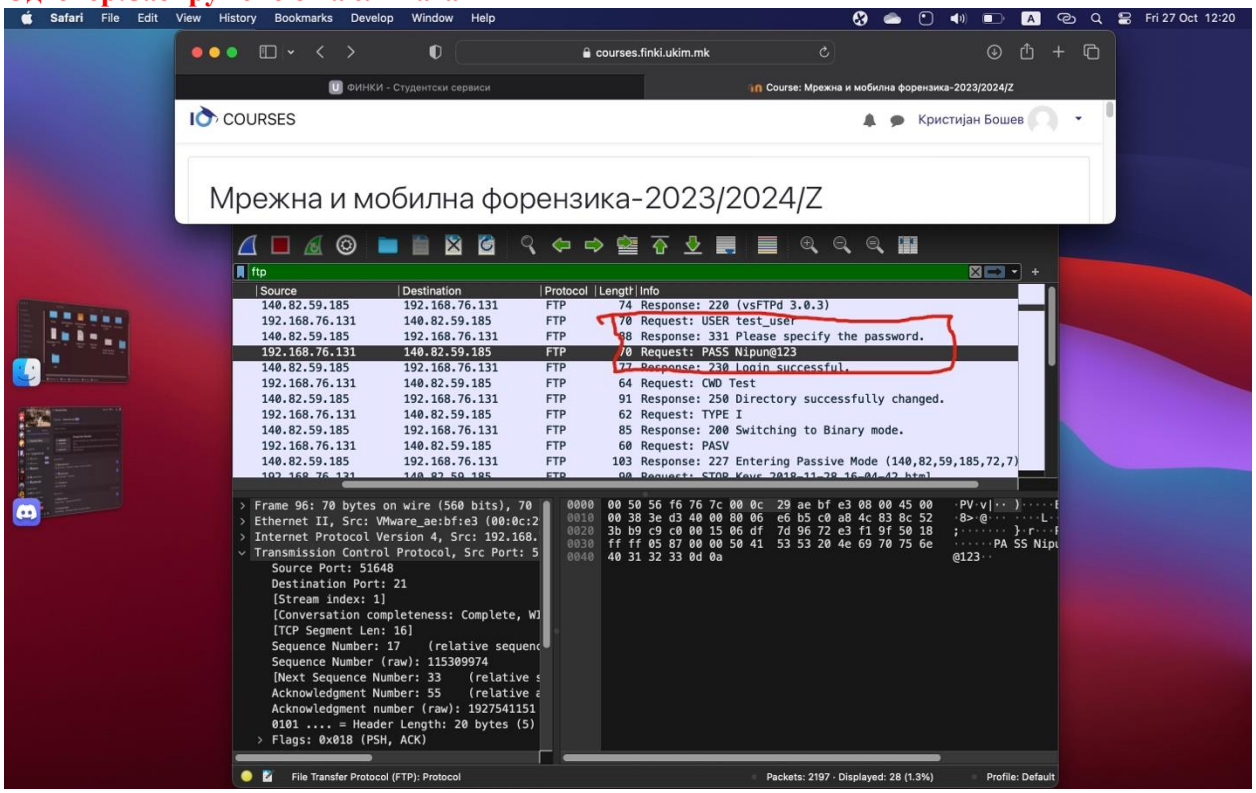
3. Која е IP адресата на FTP серверот? Пробајте да добиете дополнителни информации за неа со пасивно истражување на интернет, без директно да се поврзете. **Одговор: Заокружено е на**

сликата

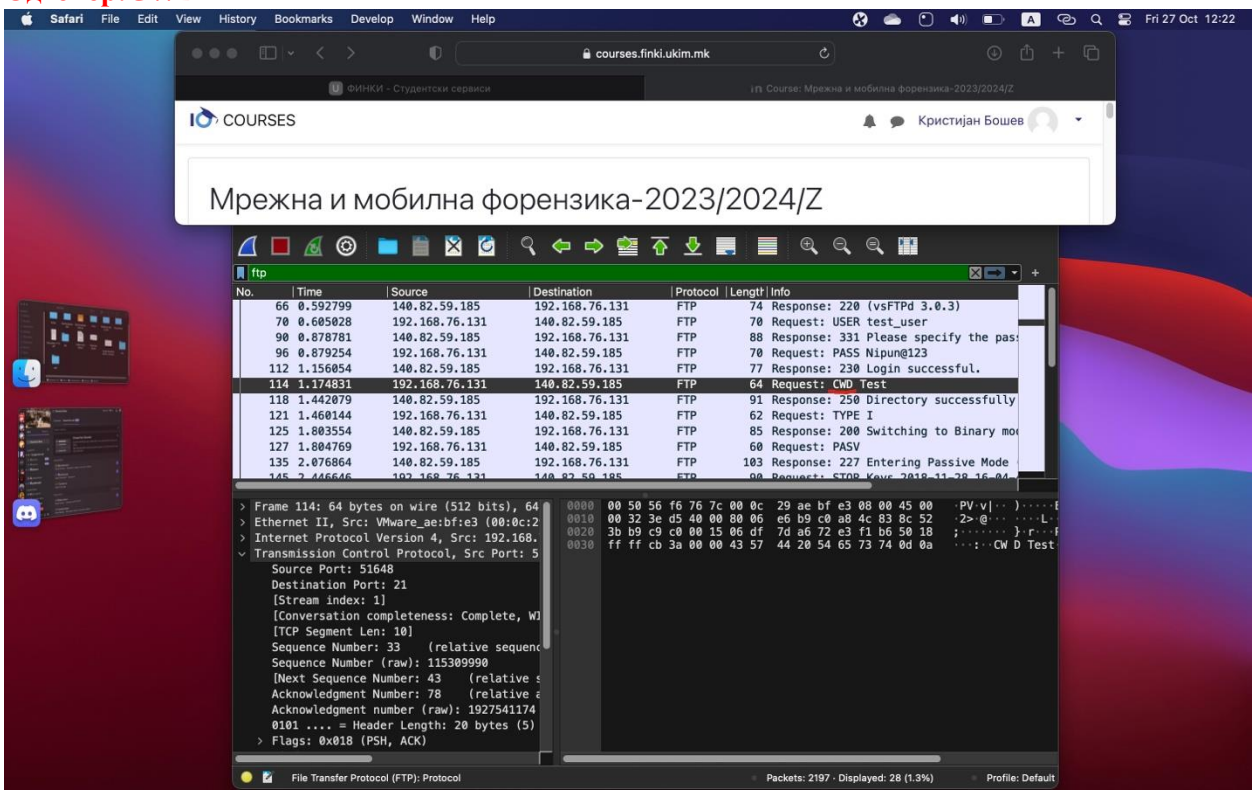


4. Кои се FTP корисничкото име и лозинка кои биле користени за најава на FTP серверот?

Одговор:Заокружено е на сликата



5. Која FTP операција е извршена?
   Одговор:CWD

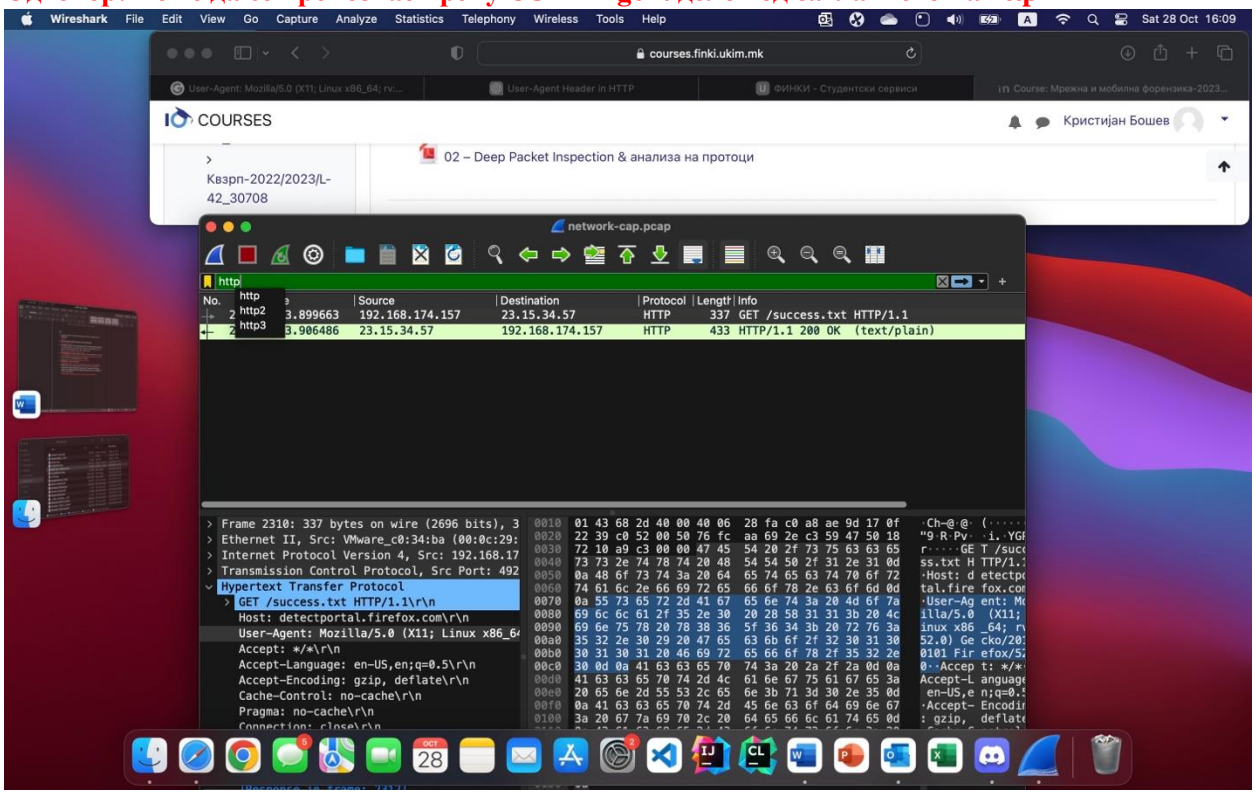


6. Која е содржината на пренесените датотеки? Како откривте?
   Одговор: Два HTML документи за ВЕБ и KEYS, може да се види и преку полето Store во Wireshark и преку Network Miner
7. Обидете се да го откриете името на keylogger софтверот кој бил инсталиран на компјутерот на вашиот шеф.
   Одговор:
8. Дали некои датотеки се од интерес? Кои? Која е нивната содржина?
   Одговор:HTML document(hands on network forensics),WEB

9.
   9.1. IP адреса на нападнатиот систем:
   9.2. IP адреса на серверот каде што се праќаат информациите: 192.168.76.131
   9.3. Колку често (во секунди) е контактиран оддалечениот сервер: 2
   9.4. Кои се информации се пренесуваат до оддалечениот сервер: Датотеки најчесто
   9.5. Листа на датотеки кои биле разменети со оддалечениот сервер (внесете ги само имињата, не е потребна самата содржина на датотеките).
      9.5.1.Keys.html
      9.5.2.WEB.html
10. Истражете самостојно некоја од дополнителните опции на NetworkMiner и накратко опишете ја. Направете куса споредба помеѓу Wireshark и NetworkMiner. Во кои ситуации би го користеле кој софтвер?
    Одговор:Нивниот софтвер и намена е доста сличен,Network Miner повеќе се користи кога има во прашање automatic extraction исто така и мејлови, а додека wireshark е подобро да се користи каде што има manual extraction

Дел 2

1. Излистајте ги резултатите. Дали забележувате некоја невообичаена активност? Како ја препознавте?
   Одговор:Може да се препознае преку USER-Agent делот од заглавието на http



2. Кои се сомнителните IP адреси? За каков тип на напад станува збор?
   Одговор:192.168.174.157
3. Кои сè адреси имаат пристапено до веб страницата http://192.168.174.142? Дали некоја (или сите) од овие одговара на сомнителните адреси од прашање 2? (Не заборавајте дека во моментов ги гледате логовите од перспектива на proxy серверот.)
   Одговор:има пристапено само 192.168.174.254 адресата и не е дел од сомнителната адреса
4. Кои сè хостови имаат пристапено до овој веб сервер? Кога? Кои страници ги имаат посетено?
   Одговор:Има пристапено само сомнителната адресата 192.168.174.157
5. Со кого и на кои порти комуницира сомнителната IP адреса?
   Одговор:49234 i 80
6. Образложение на намената на портите.
   Одговор:Едната порта ја користи како изворна порта, а другата како дестинациска
7. Образложете го нападот и дадете опционална слика. Опфатете зошто во прашање 2 изгледаше како нападот да потекнува од proxy серверот. Од каде всушност потекнува нападот? Како е изведено маскирањето? Дадете претпоставка за начинот на пробивање на машината 192.168.174.157.
   Одговор: Преку mozzila пребарувач кој што работи на linux и на крај се добива порака success