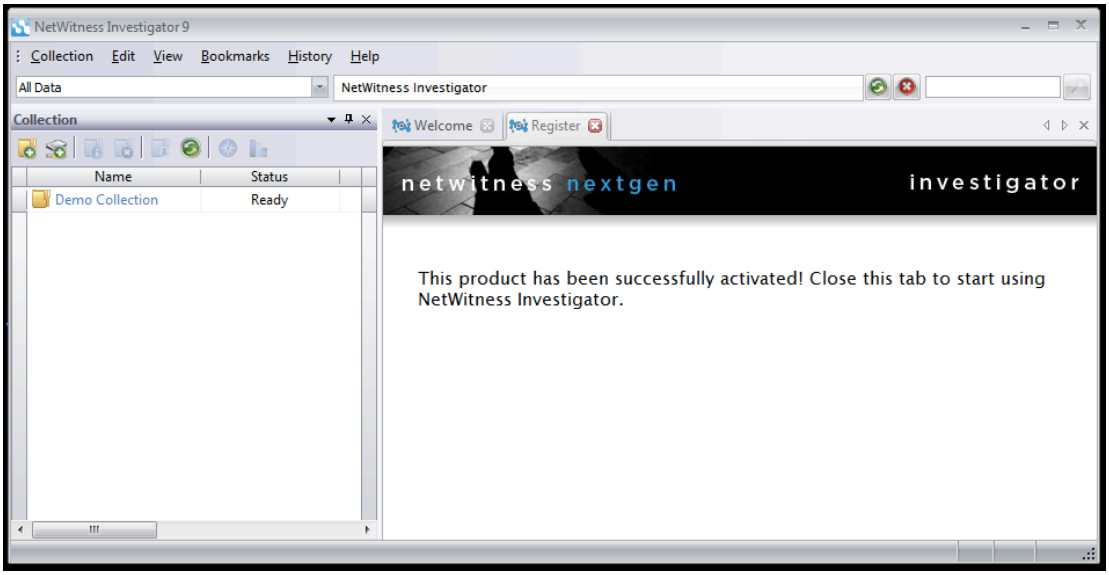
Project 17: NetWitness (15 pts.)

Kebutuhan Project

- Komputer Windows. Pada tutorial ini menggunakan Windows 7 virtual machine.

Menginstal NetWitness

1. Buka browser dan arahkan ke http://www.emc.com/security/rsa-netwitness.htm#!freeware
    a. Click "**Download NetWitness Investigator Freeware**"
    b. Isi form dan click **Submit**. Bisa di download juga di elearning
    c. Download file **NwInvestigatorSetup.exe** dengan ukuran (131 MB).
    d. Install software dengan default options.
    e. Buka desktop, double-click icon "**NetWitness Investigator 9.6**".
    f. Jendela "NetWitness Investigator 9" terbuka. Kotak pop up, berisi pesan "Revocation information for the security certificate for this site is not available...".
    g. Click **Yes** untuk mem-bypass pesan.
    h. Isi form registrasi.
    i. Check email untuk product activation code. Ikuti instruksi di email untuk mengaktifkan NetWitness.
    j. NetWitness sekarang sudah aktif, seperti berikut:



    k. Tutup tab Register.

Menginstal Wireshark

2. Jika di komputer belum ada Wireshark, bisa di download di http://www.wireshark.org/
3. Jalankan Wireshark. Pilih network adapter yang terkoneksi ke Internet

Mengumpulkan Evidence

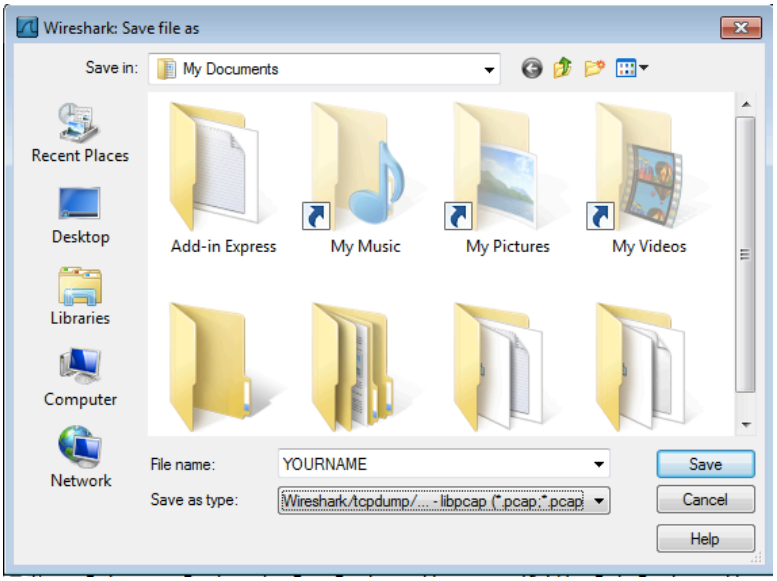
4. Open a Web browser and do these things:

a. Go to http://id.wikipedia.org/ and log in with the user name **Fccf** and a password of **foresec**

b. Pada Wikipedia, masuk ke Portal Sumatera dan loading halaman mengenai portal Sumatera.

c. Buka halaman: http://elearning.binadarma.ac.id.

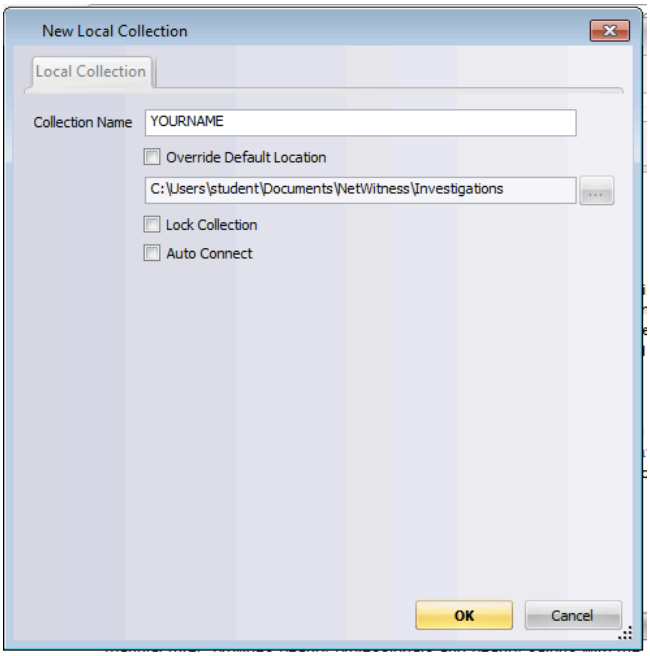
d. Stop packet capture. Simpan file packet capture dengan nama **YOURNAME** dan jenis file gunakan "**Wireshark/tcpdump/ ... -libpcap (*.pcap)**", seperti berikut:



Mengimport Evidence ke NetWitness

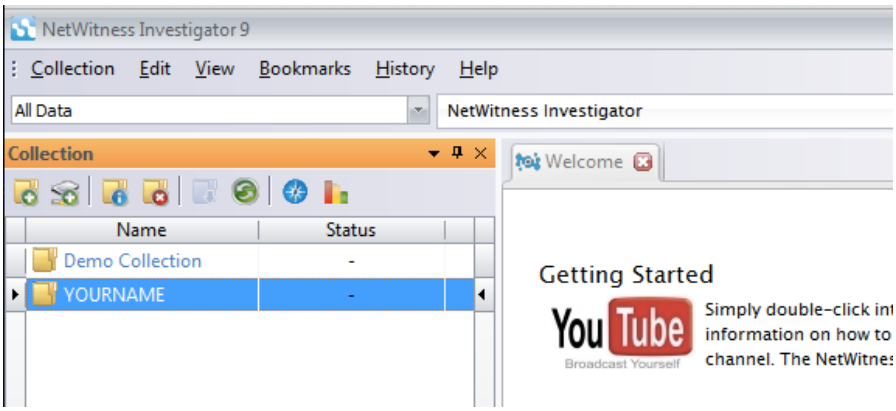
5. Di NetWitness, dari menu bar, click **Collection**, "**New Local Collection**".

a. Masukkan Collection Name berupa **YOURNAME** (gunakan nama masing-masing, seperti berikut:



b. Click **OK**

c. Pada panel kiri NetWitness, double-click **YOURNAME** seperti berikut:



d. Status harus memperlihatkan "Connecting", dan setelah beberapa detik, berubah menjadi "Ready".

e. Di NetWitness, dari menu bar, click **Collection**, "**Import Packets**".

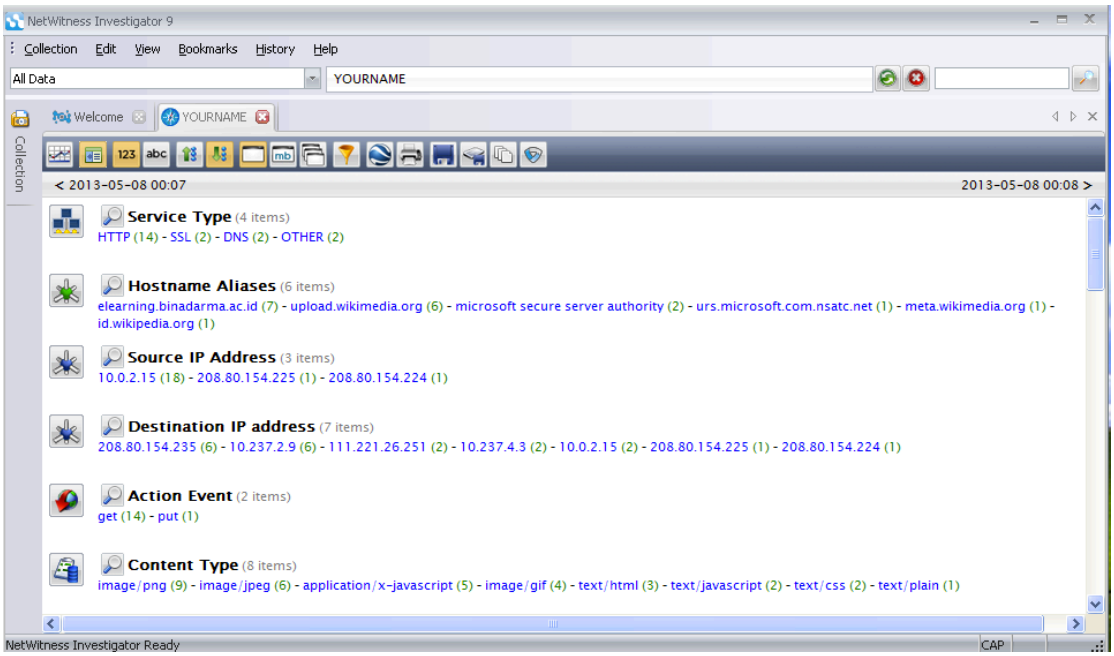
f. Arahkan ke file **YOURNAME.pcap** dan double-click it.

g. Status field memperlihatkan progress--, 1%, kemudian 99%, kemudian Done.

Menganalisis Evidence

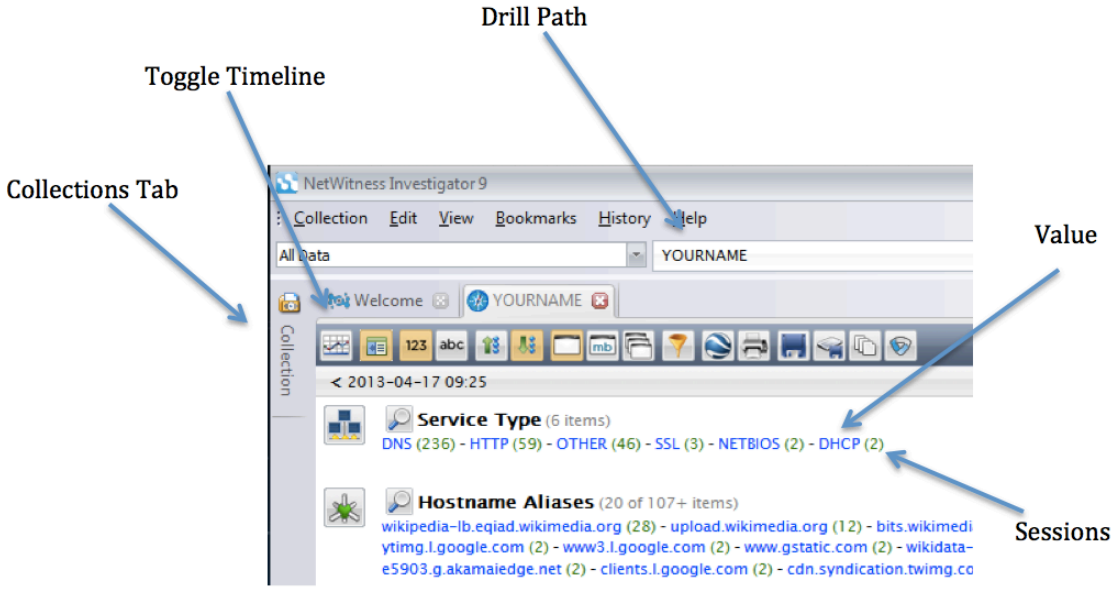
6. Pada Collections pane NetWitness, double-click kembali **YOURNAME**.

a. Report muncul, memperlihatkan daftar jenis trafik, seperti berikut.



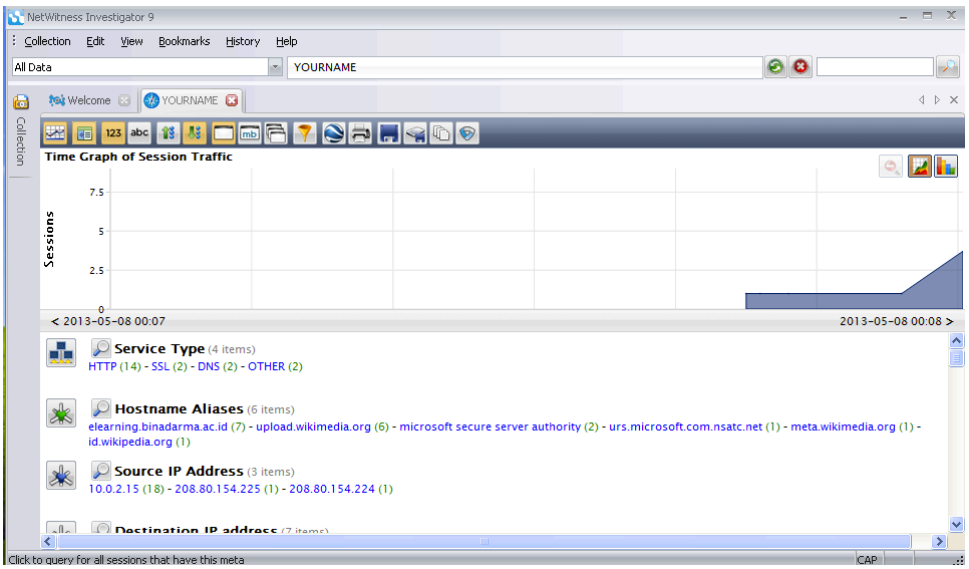
b. Items memperlihatkan shown below:

- Tab **Collections Tab**
- Tombol **Toggle Timeline** memperlihatkan grafik data
- **Drill Path** memperlihatkan filters yang digunakan untuk menghilangkan data yang tidak penting—data yang akan kita cari pada YOURNAME collection.
- Pada Report, pasangan entries muncul: **Value** diikuti dengan nomor **Sessions** di parentheses, missal DHCP (2).



c. Click tombol **Toggle Timeline** memperlihatkan Timeline, seperti berikut.

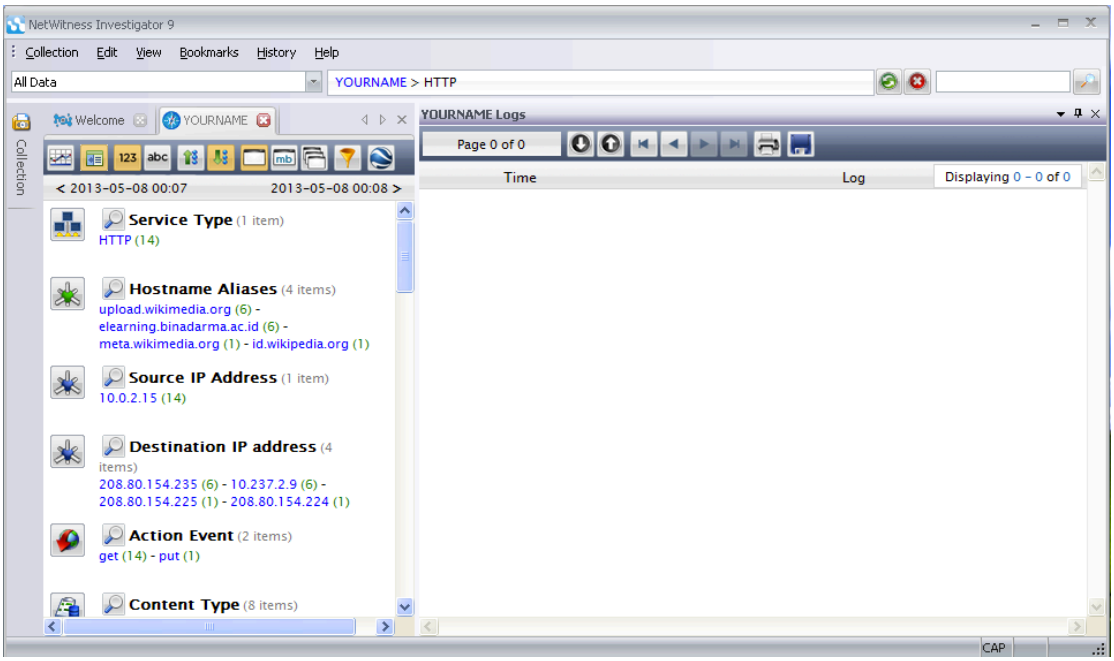
d. Timeline memperlihatkan traffic dalam bentuk grafik, dan bisa digunakan untuk meperlihatkan dalam interval waktu tertentu. Dalam project ini toggle timeline tidak digunakan, jadi click tombol **Toggle Timeline** lagi untuk menyembunyikannya.



Mencari Wikipedia Login

7. Pada bagian Report, pada bagian atas berjudul "Service Type", click link biru **HTTP**.

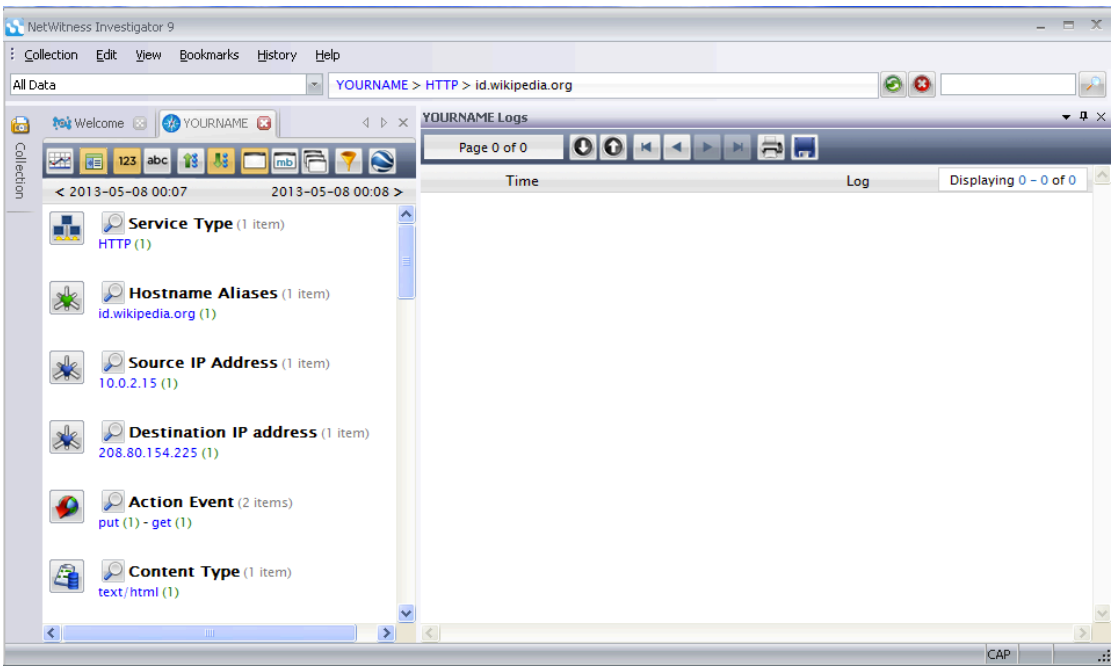
   a. Filter ini mengeluarkan semua non-HTTP traffic. Perhatikan Drill Path berubah menjadi "YOURNAME > HTTP", seperti berikut:



b. Setengah bagian jendela sebelah kanan memperlihatkan Log panel yang kosong. Jika kita memiliki log files di dalam collection, hal ini akan sangat membantu, akan tetapi dalam kasus ini data hanya berisi file PCAP tanpa logs, jadi panel ini tidak membantu.

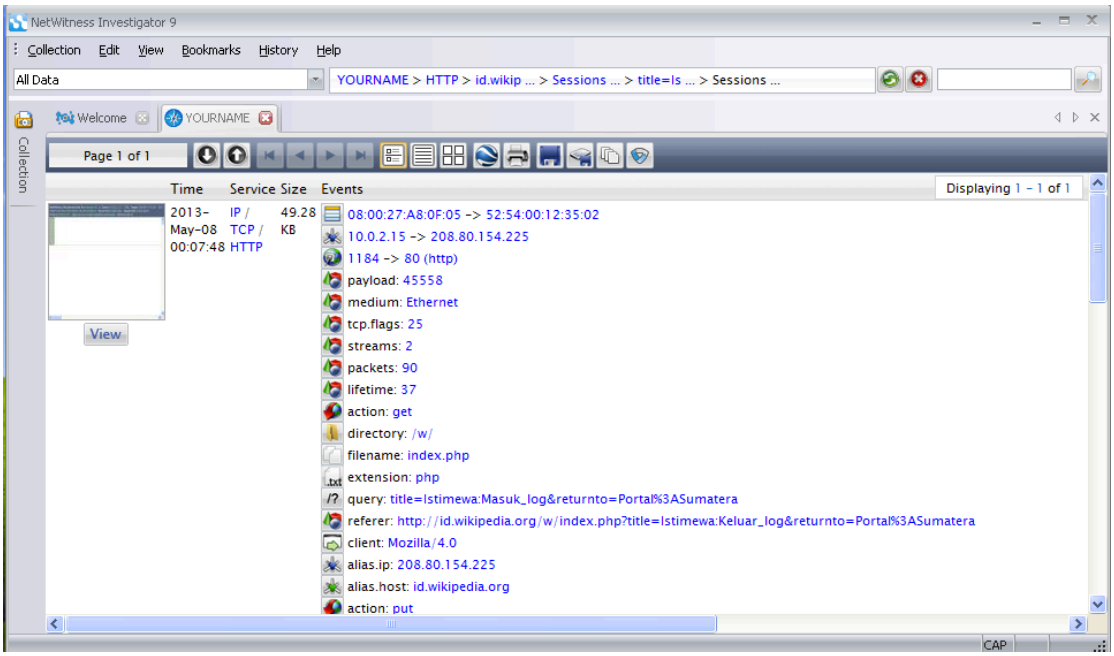
c. Pada bagian Report, pada bagian judul kedua "Hostname Aliases", click link biru **id.wikipedia.org**.

d. Filter ini membuang semua trafik ke hosts lain. Perhatikan Drill Path berubah menjadi "YOURNAME > HTTP > id.wikipedia.org", seperti berikut:

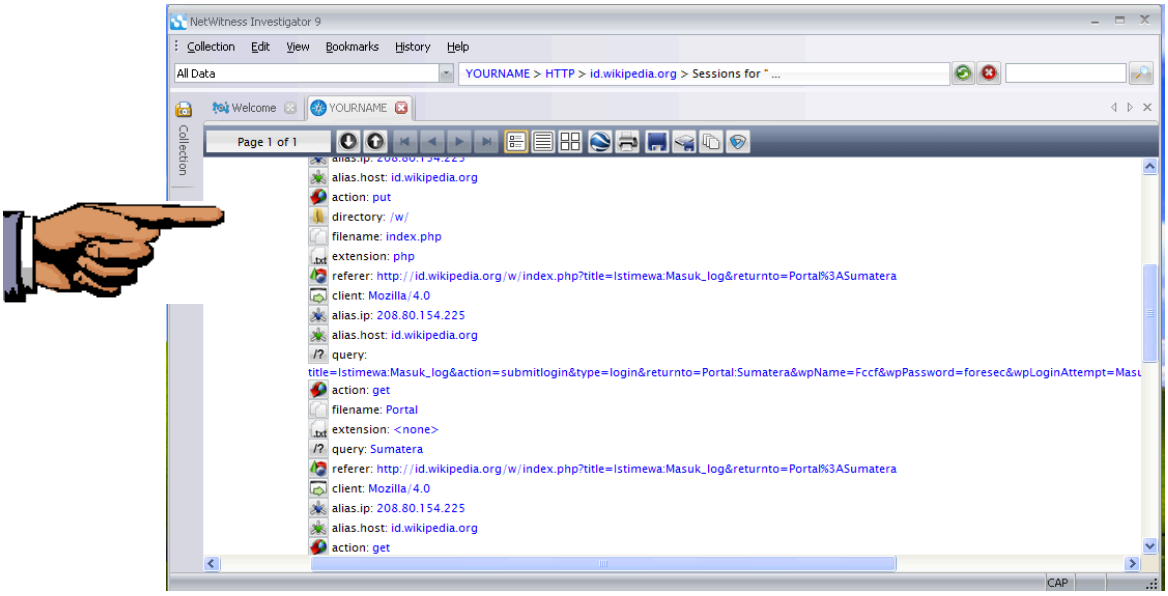


e. Sekarang click angka biru dalam kurung di sebelah kanan id.wikipedia.org – dalam contoh "1". Angka yang ditunjukkan bisa jadi berbeda.

f. Bagian ini memperlihatkan sessions dengan banyak details, seperti terlihat di bawah. Panel og di sebelah kanan hanya menghabiskan tempat – tutup dengan meng-click tombol X.



g. Scroll down dan cari "**Password=foresec**", sperti berikut:

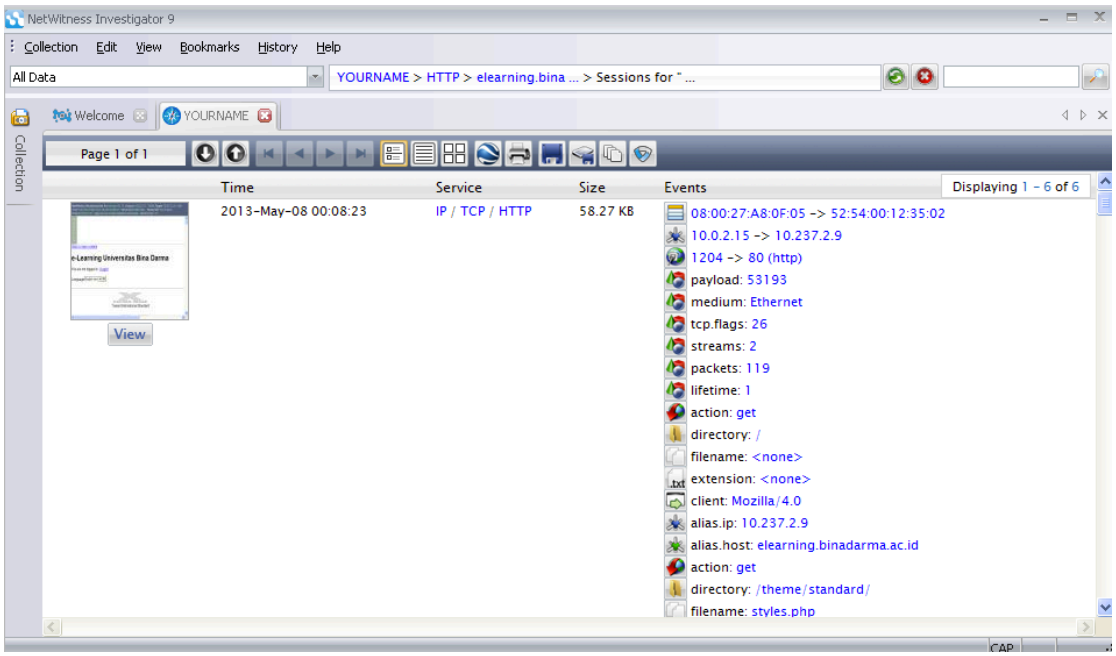


Simpan Screen Image

8. Pastikan "**Password=foresec**" terlihat.
9. Tekan PrintScrn. Simpan keseluruhan gambar desktop dengan nama "**NamaKamu_Proj17a"**.

Menampilkan Rekonstruksi

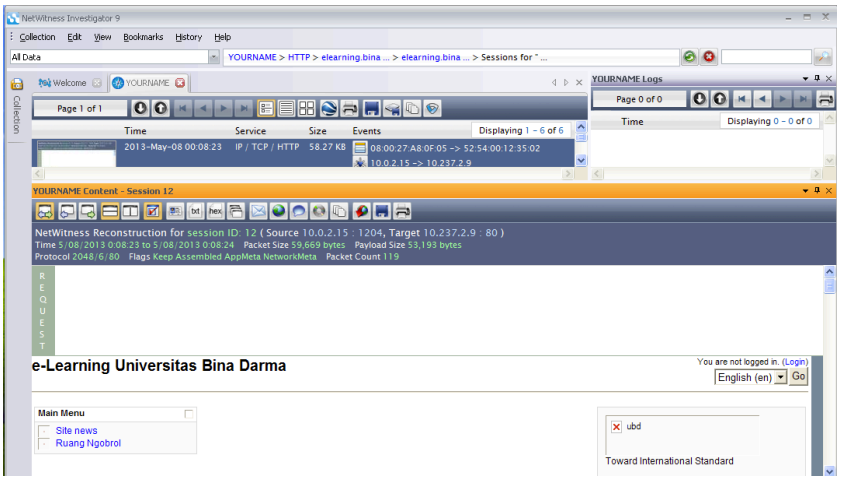
10. Pada bagian atas tengah jendela NetWitness, pada Drill Path, click **HTTP**.
    a. Pada bagian "Hostname Aliases", click **elearning.binadarma.ac.id**
    b. Pada bagian "Hostname Aliases", click angka di sebelah kanan "elearning.binadarma.ac.id "—dalam contoh, angka **6**
    c. Sekali lagi, Logs panel --ditutup.
    d. HTTP sessions dengan server elearning.binadarma.ac.id tampil, seperti berikut:



e. Pada sisi kiri Report untuk tiap session, terdapat icon yang memperlihatkan bagaimana tampilan halaman Web, dengan tombol **View** berwarna abu-abu.

f. Click tombol **View**.

g. Maka akan terlihat "NetWitness Reconstruction" halaman dari packets, sperti berikut:



Simpan Screen Image

11. Pastikan header "e-learning Universitas Bina Darma " terlihat.

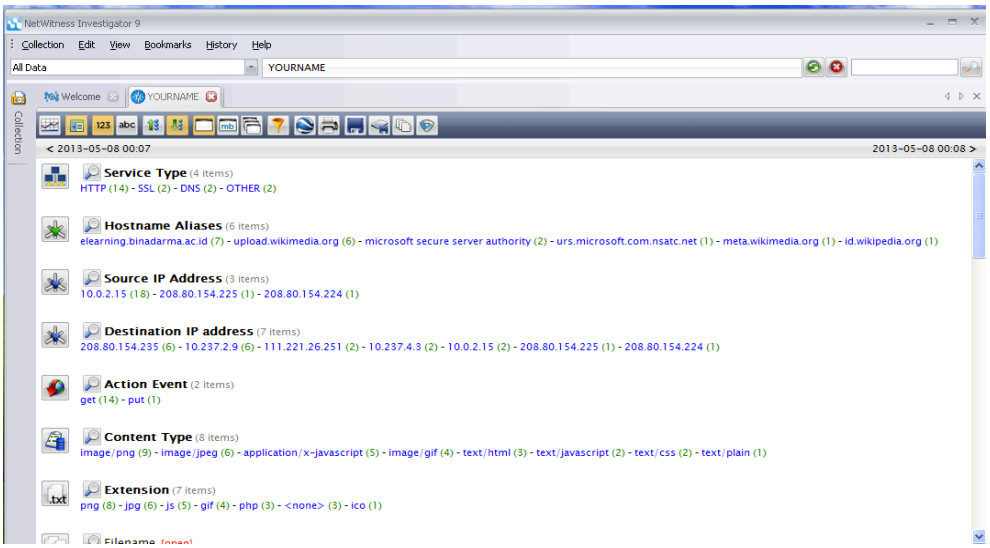
a. Tekan PrintScrn key. Simpan keselurhan desktop image dengan nama **"NamaKamu_Proj17b"**.

b. Tutup panel "NetWitness Reconstruction" dengan meng- click tombol X.

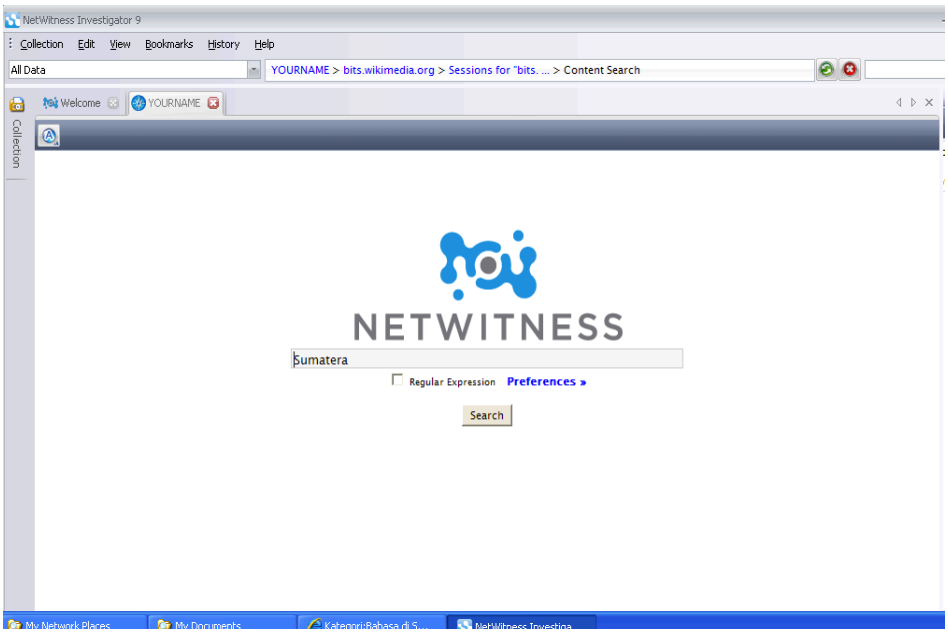
Pencarian

12. Pada bagian atas jendela NetWitness, pada Drill Path, click tulisan biru **YOURNAME**.

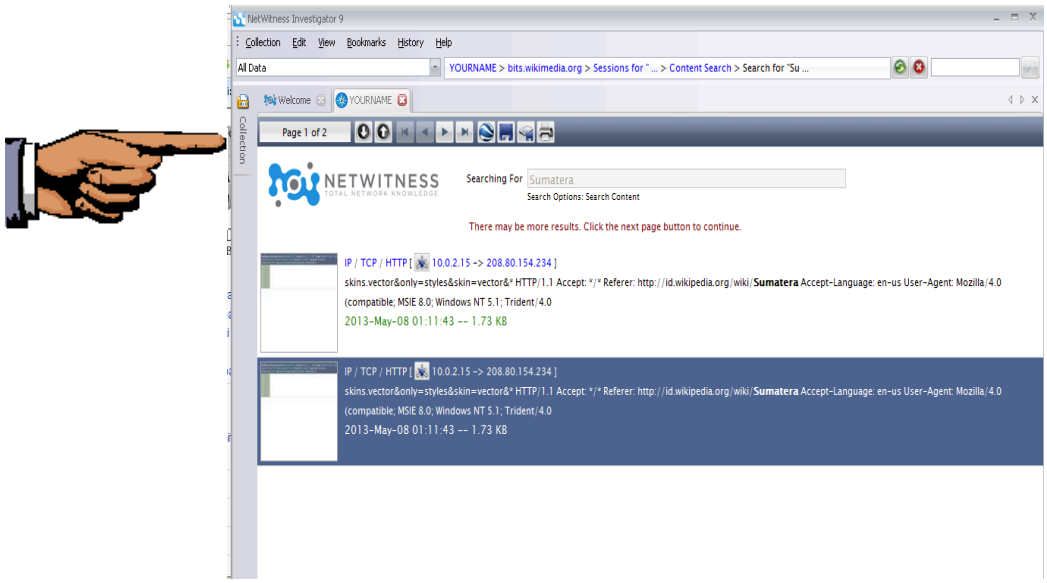
a. Pada sebelah kanan jendela, di baris yang sama dengan "YOURNAME", click icon kaca pembesar di sudut kanan atas, seperti berikut:



13. Pada kotak pencarian, ketikkan **Sumatera** seperti berikut. Click tombol **Search**.



14. Maka akan tampil report, memperlihatkan hasil pencarian, dengan thumbnails halaman di sisi kiri seperti berikut:



15. Tekan tombol prinscreen untuk mengkopi seluruh desktop. Simpan dengan nama "NamaKamu_Project17c".
16. Click thumbnails untuk melihat Reconstruction halaman.

Mengumpulkan Project

17. Kirim melalui elearning.

Last modified 5-8-13