**Lab 11: Investigating browser history**

**What You Need for this lab**

* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
    - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
  + Image “cfreds\_2015\_data\_leakage\_pc.dd” from Lab 5

**Goals**

* Understand the application layer of a computer system that generates evidence
* Understand the behavioral model of an application
* The approach to investigating browser history (evidence generated by an application)
* Familiar with important tools for browser investigations

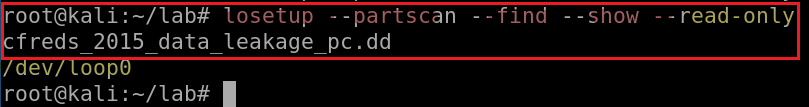
**Step 1**

* Set up loop device (a pseudo-**device** that makes a file accessible as a block **device**)

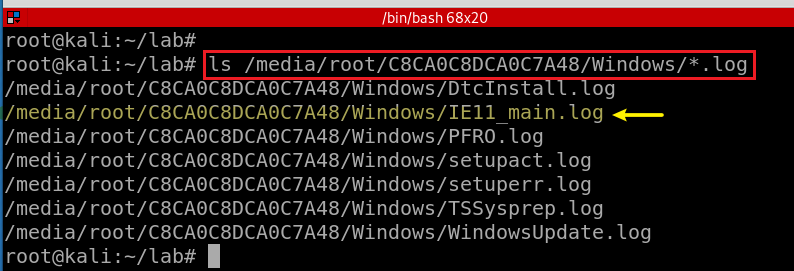
*losetup --partscan --find --show --read-only cfreds\_2015\_data\_leakage\_pc.dd*

*mkdir /mnt/loopdev*

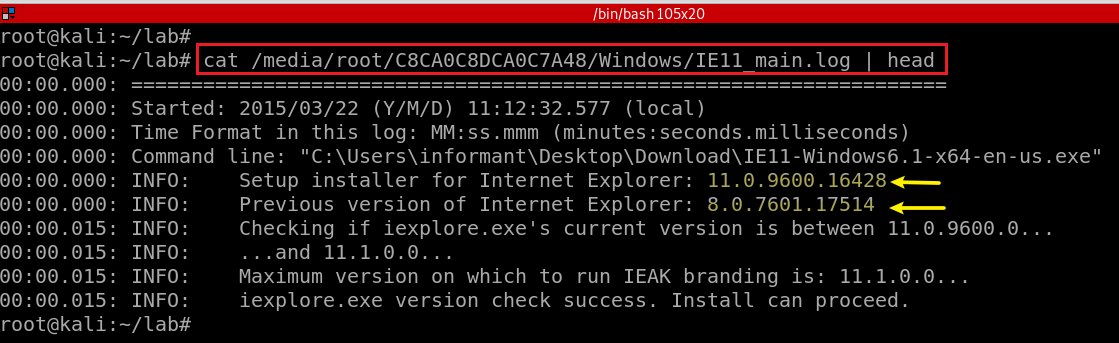
*mount -o ro,loop,offset=206848 cfreds\_2015\_data\_leakage\_pc.dd /mnt/loopdev*



* Check all versions of IE via .log



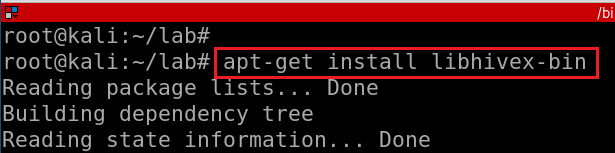
* Exam IE logs



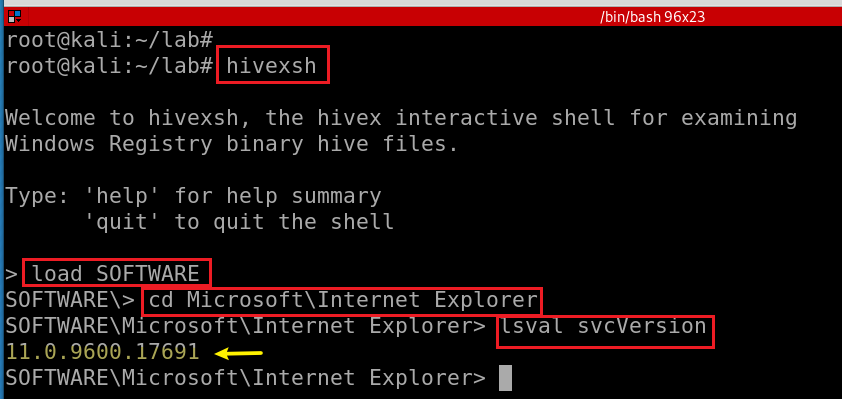
* **Can you find the version number?**

Use Windows Registry hive shell (*hivexsh*)

* Install *hivexsh*

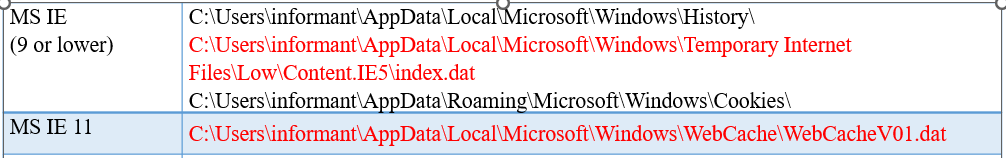


* Exam the version of IE using *hivexsh*

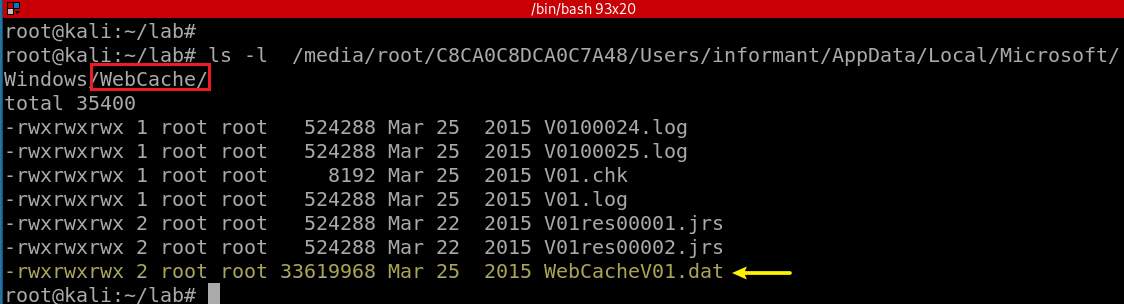


**Step 2.**

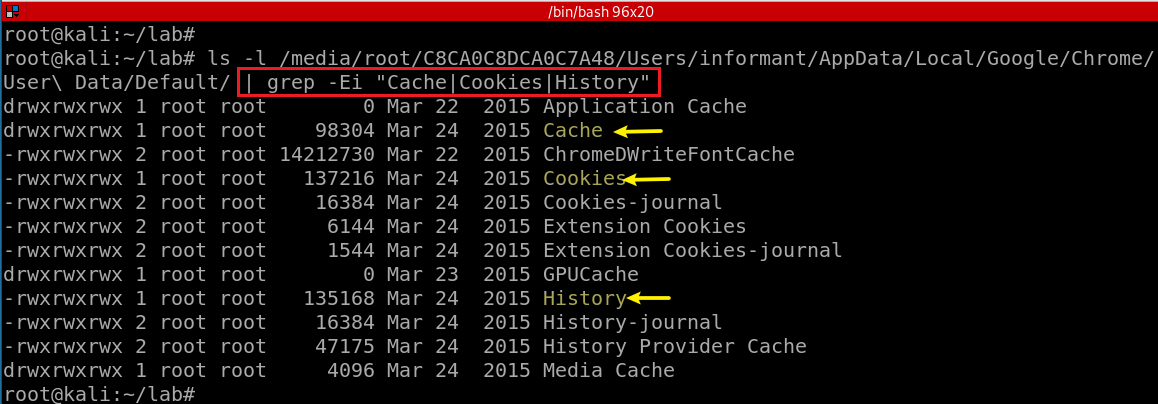
Identify directory/file paths related to the web browser history



* Internet Explorer 11 History



* Find Google Chrome Cache, Cookies, and History



**What websites were the suspect accessing? (Timestamp, URL...)**

* + Get browser history files
  + View these files

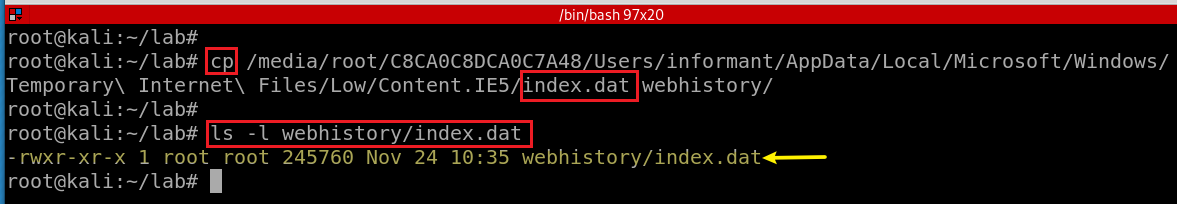
**Step 1.**

Copy Three Browser History Files

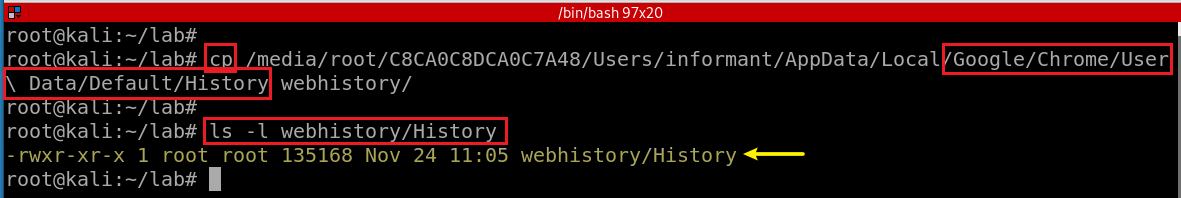
Copy IE 11 History



Copy IE 8 History



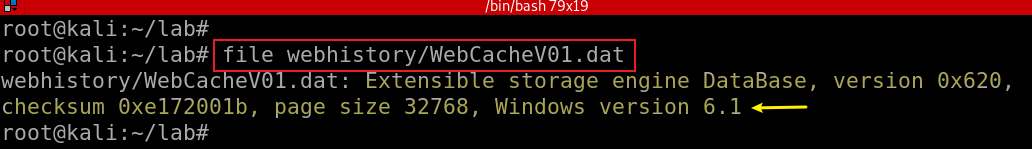
Copy Chrome History



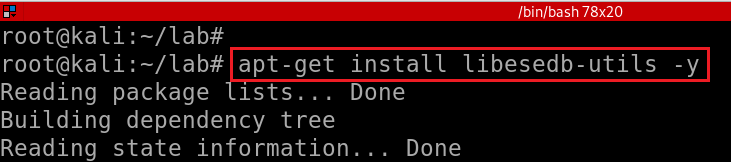
**Step 2.**

View IE 11 History Using *libesedb*

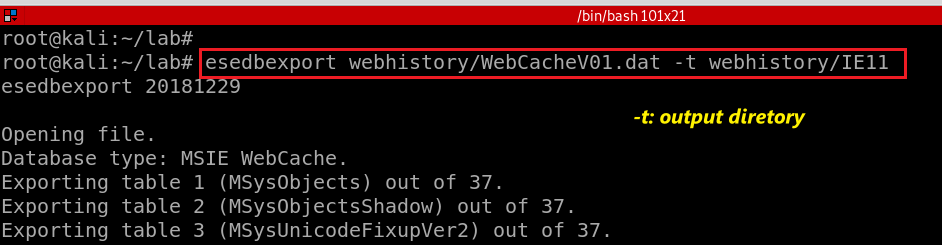
Find the file type of *WebCacheV01.dat*



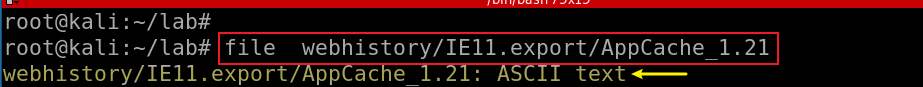
* Install *libesedb*



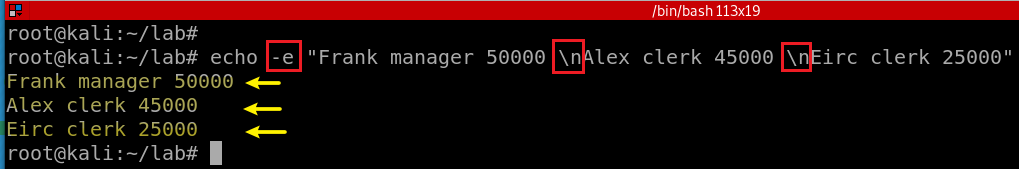
* Export *WebCacheV01.dat* to the folder webhistory/IE11



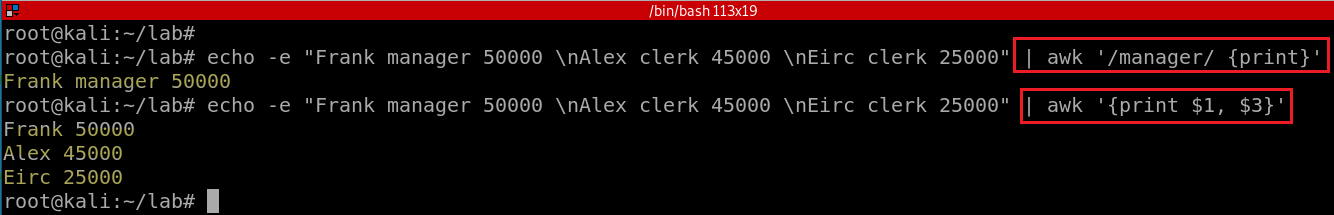
* Find the type of the file



* Create three lines with three attributes

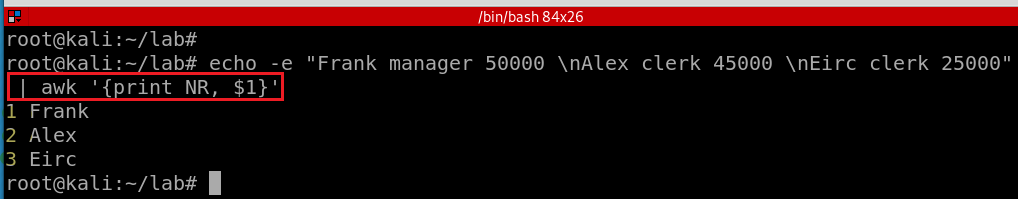


* Select lines with the key word “*manager*”
* Select attributes 1 and 3



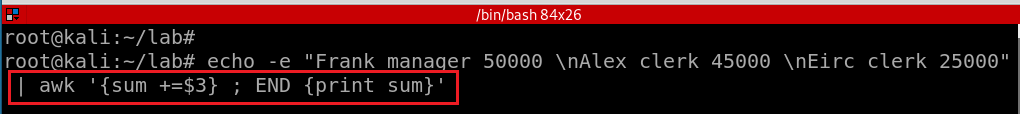
* Show Row Number

*echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{print NR, $1}‘*

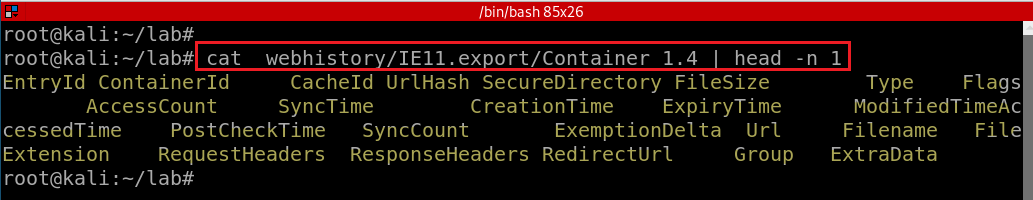


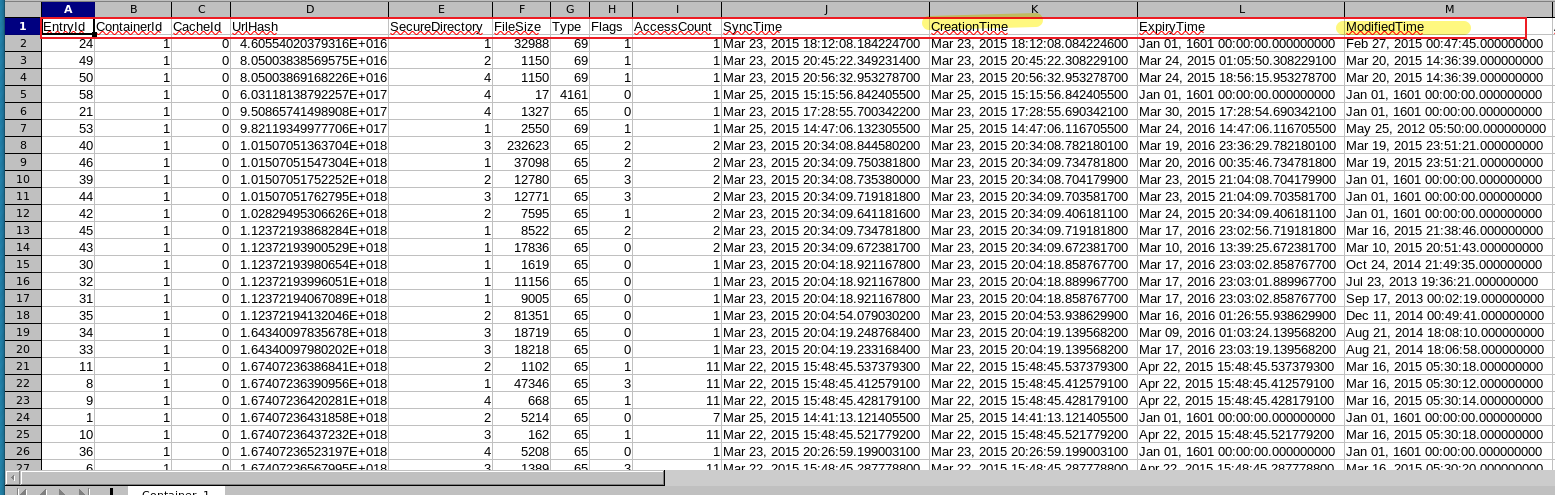
* Calculate sum

*echo -e "Frank manager 50000 \nAlex clerk 45000 \nEirc clerk 25000" | awk '{sum +=$3} ; END {print sum}'*



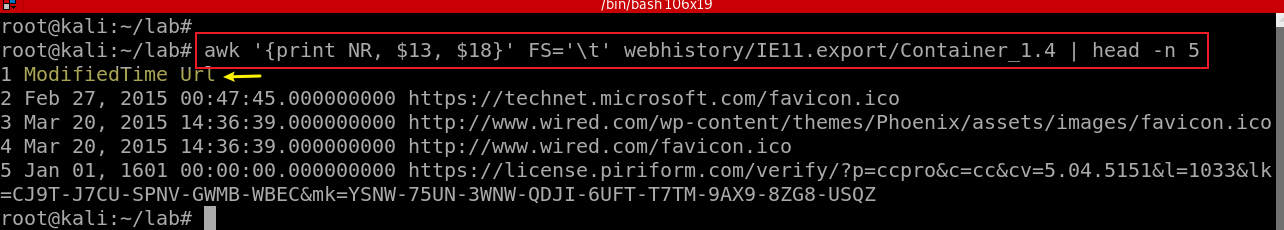
* Show field names





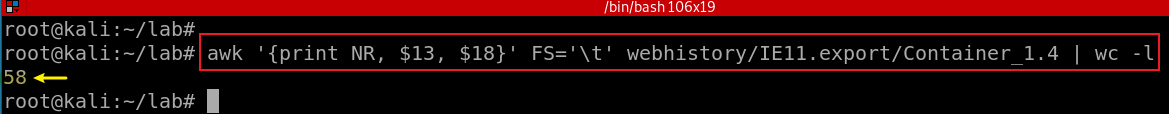
* Separate fields with tab *‘\t’* and show *ModifiedTime* and *URL*

*awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container\_1.4 | head -n 5*



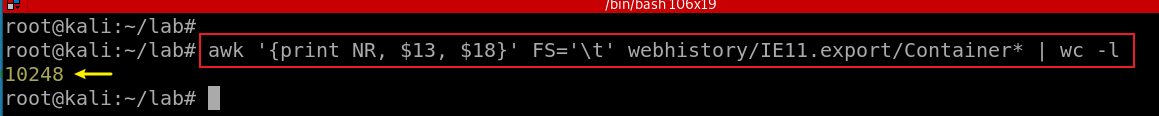
* Count the number records in the file

*awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container\_1.4 | wc –l*



* Count the number records in all files start with the string “*Container*”

*awk '{print NR, $13, $18}' FS='\t' webhistory/IE11.export/Container\* | wc -l*



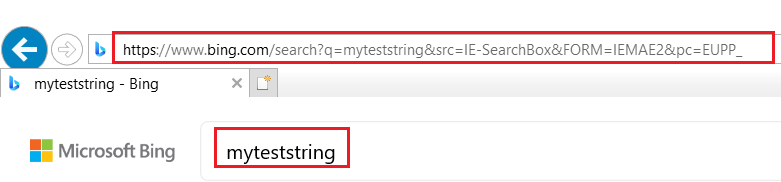
**Step 3.**

List all search keywords using web browsers. (Timestamp, URL, keyword...)

* IE browser

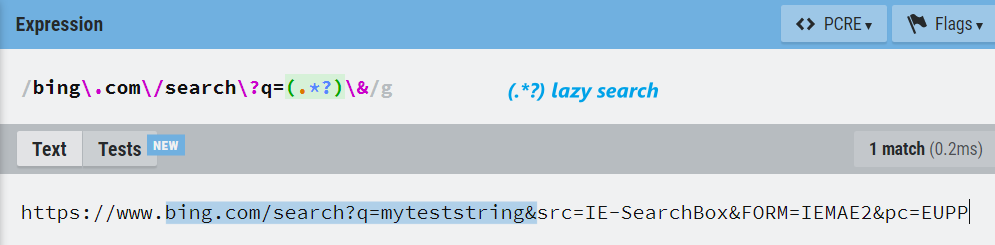
**Web Query String**

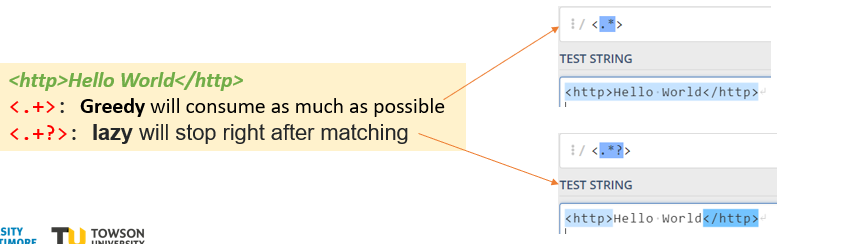
https://www.bing.com/search?q=myteststring&src=IE-SearchBox&FORM=IEMAE2&pc=EUPP



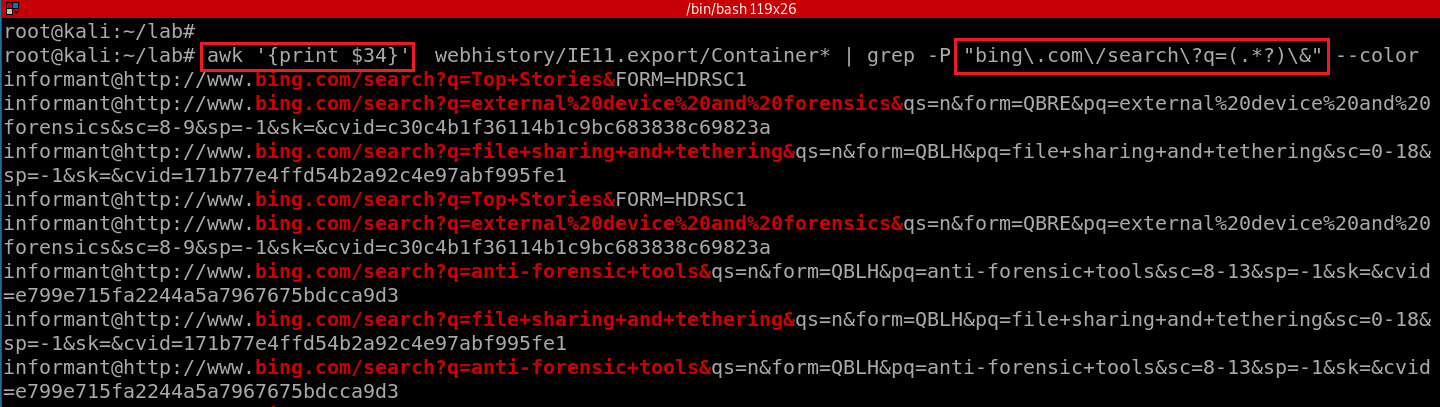
* Regular expression for bing.com search

<https://regexr.com/>





* List IE 11 search keywords



**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 11.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 11 From YOUR NAME**", replacing "YOUR NAME" with your real name.