



Open Source Digital Forensics Conference  
DECEMBER 1, 2021 • VIRTUAL



# FORENSIC ACQUISITION OF WEBSITES, WEBPAGES AND ONLINE SERVICES WITH OPEN SOURCE TOOLS

---

“FREEZING” ONLINE EVIDENCE: A NEW CHALLENGE IN DIGITAL FORENSICS

Paolo Dal Checco – Digital Forensics Expert





# WHO AM I

---

- Ph.D. in Computer and Networks Security, University of Turin
- Digital Forensics Expert (10+ years, 2k+ digital forensics cases)
- Expert Witness in Court for Public Prosecutors, Judges and Law Enforcement
- Consultant for Private Sector, Companies and Law Firms
- Interests in Mobile Forensics, Cryptography, Cryptocurrency Forensics, OSINT
- Contract teacher in masters and training courses for University of Torino, Milano, Genova



## FOCUS: ONLINE EVIDENCE

---

- Acquiring and preserving digital evidence from hard drives, smartphones or pendrives is pretty straightforward by now
- What about online evidence?
  - Websites, webpages, cloud, tweets, social profiles or whatever is found on the Internet
- Few tools and services around, both commercial and free, some are good for webpages and other for websites, some can be adapted to different scenarios
- No standard or comprehensive solution



## STATE OF THE ART: LOCAL TOOLS (FREE)

---

- MAGNET Web Page Saver ([www.magnetforensics.com/resources/web-page-saver](http://www.magnetforensics.com/resources/web-page-saver))
- ArchiveWeb.page Desktop App/Chrome Plugin ([archiveweb.page](http://archiveweb.page))
- Browsertrix Crawler ([github.com/webrecorder/browsertrix-crawler](https://github.com/webrecorder/browsertrix-crawler))
- PyWb ([pywb.readthedocs.io/en/latest/](http://pywb.readthedocs.io/en/latest/))
- OSIRT (more OSINT than forensics)
- Wget/HTTrack (not that much forensic tools)
- Etc...



## STATE OF THE ART: LOCAL TOOLS (COMMERCIAL)

---

- Forensic Acquisition of Websites - FAW ([www.fawproject.com](http://www.fawproject.com))
- XI Social Discovery ([www.xi.com/products/xi-social-discovery](http://www.xi.com/products/xi-social-discovery))
- Hunchly Chrome Plugin ([www.hunch.ly](http://www.hunch.ly))
- Paliscope Chrome Plugin ([www.paliscope.com](http://www.paliscope.com))
- WebPreserver/PageFreezer Chrome Plugin ([www.webpreserver.com](http://www.webpreserver.com))
- Etc...



## STATE OF THE ART: SERVICES (FREE)

---

- Web Archive ([web.archive.org](http://web.archive.org))
- Archive.Today ([archive.today](http://archive.today))
- Conifer - Collect and revisit web pages ([conifer.rhizome.org](http://conifer.rhizome.org))
- Legalizer ([www.legalizer.it](http://www.legalizer.it))
- Etc...



## STATE OF THE ART: SERVICES (COMMERCIAL)

---

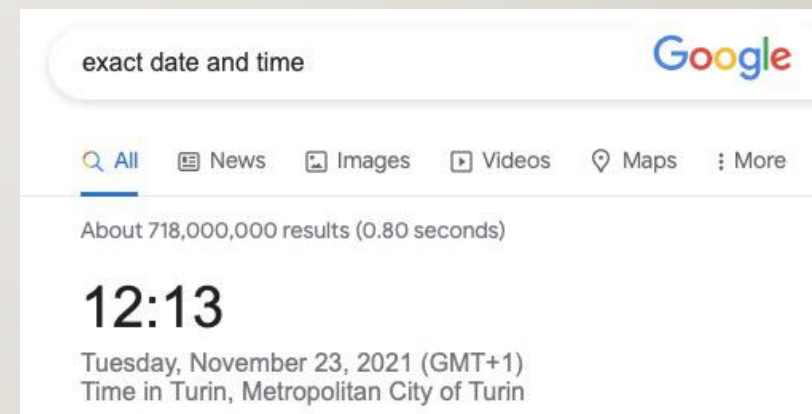
- LegalEye ([www.legaleye.it](http://www.legaleye.it))
- Giuffré Cliens Prova Digitale ([provadigitale.cliens.it](http://provadigitale.cliens.it))
- CRIO Solutions ([criosolutions.com](http://criosolutions.com))
- Harvard Perma.cc ([www.perma.cc](http://www.perma.cc))
- Kopjra Web Acquisition ([acquisition.kopjra.com](http://acquisition.kopjra.com))
- TrueScreen
- Web Freeze by eWitness ([www.ewitness.eu/web-freeze](http://www.ewitness.eu/web-freeze))
- VeriFact ([www.verifact.com.br](http://www.verifact.com.br))
- Etc...



# THE BASE CONCEPTS OF WEB ACQUISITIONS

---

- The idea: make web acquisitions as “valid” and “court accepted” as traditional acquisitions
- ISO/IEC 27037 compliant (Principles of Chain of Custody, etc...)
- Document every step by recording and crossing:
  - Video Stream
  - Network Traffic (with SSL keys)
  - DNS, Traceroute, NTP, etc...
  - Time Reference (visit real time news websites + time&date)
- Pack and timestamp Acquisition (Blockchain, CA, etc...)







# THE IDEA BEHIND THE PROJECT

---

- Create a Linux Virtual Machine (Ubuntu, Lubuntu, Debian, etc...)
- Visit Webpage
- Crawl Website
- Document and record every single step of the acquisition/visit
- Create a «digital forensic copy/image» of the page/visit/website
  - Just like EWF/AFF for hard drives, UFD/OFB/XRY for mobile acquisitions, etc...



# HANDS ON: SCENARIOS

---

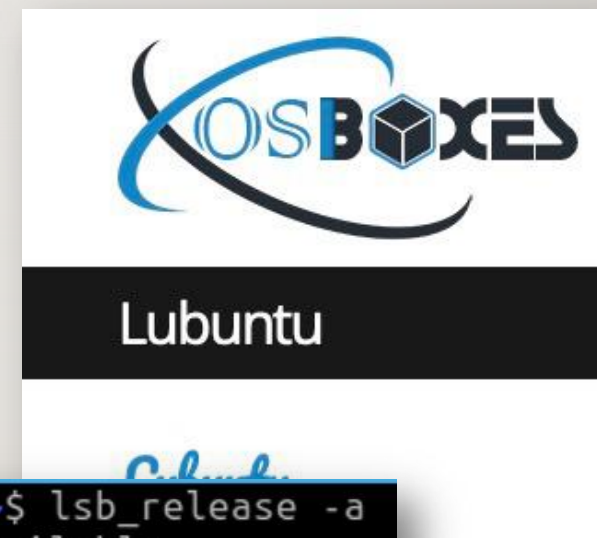
- **Automatic** Forensic Acquisition of **whole website** (via **crawler**)
  - Pros: can crawl whole websites with a click
  - Cons: some websites may result different because of AJAX/HTML5 rendering
- **Manual** Forensic Acquisition of **webpage** (via **browser**)
  - Pros: good for webpages built in browser, streaming, etc...
  - Not good for whole websites



# WEBPAGE ACQUISITION VIA BROWSER

---

- Let's download/install a Linux VM
- Install missing tools
- apt-get install python3-pip google-chrome-stable  
python3-opentimestamps ffmpeg
- pip3 install opentimestamps-client



```
labimager@labimager:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.10
Release:        20.10
Codename:       groovy
```



# WEBPAGE ACQUISITION VIA BROWSER

---

- Open a new terminal window (#1) and place it in top left part of desktop
- Create the folder for the case

```
labimager@labimager:~$ mkdir osdfcon2021  
labimager@labimager:~$ cd osdfcon2021/
```



# WEBPAGE ACQUISITION VIA BROWSER

---

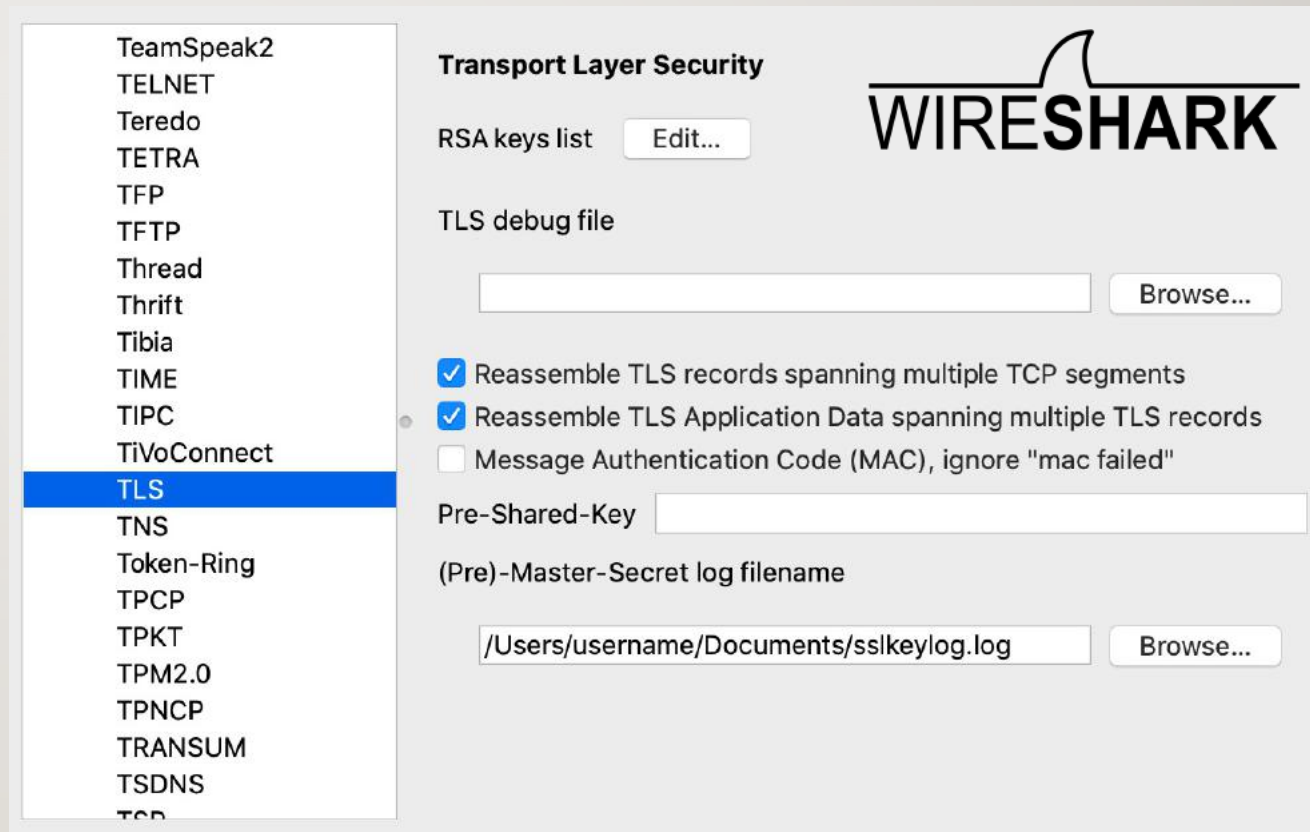
- On terminal #1 run **"script w1.txt"** to store command line history in w1.txt file
- export the SSLKEYLOGFILE path to enable libssl dumping SSL keys  
**export SSLKEYLOGFILE="/home/labimager/osdfcon2021/sslkeylogfile.log"**

```
labimager@labimager: ~/osdfcon2021
labimager@labimager:~/osdfcon2021$ script w1.txt
Script started, output log file is 'w1.txt'.
labimager@labimager:~/osdfcon2021$ export SSLKEYLOGFILE="/home/labimager/osdf
con2021/sslkeylogfile.log"
labimager@labimager:~/osdfcon2021$ echo $SSLKEYLOGFILE
/home/labimager/osdfcon2021/sslkeylogfile.log
labimager@labimager:~/osdfcon2021$
```



# WEBPAGE ACQUISITION VIA BROWSER

- SSL keys are mandatory
- In Wireshark the SSL network traffic can thus be decrypted by opening the pre-master-secret-log in TLS settings



The screenshot shows the Wireshark interface for configuring Transport Layer Security (TLS) settings. On the left, a list of protocols is displayed, with 'TLS' selected and highlighted in blue. The main panel on the right is titled 'Transport Layer Security' and contains several configuration options:

- RSA keys list:** A button labeled 'Edit...' is visible.
- TLS debug file:** An empty text input field with a 'Browse...' button to its right.
- Reassembly options:** Three checkboxes are present:
  - Reassemble TLS records spanning multiple TCP segments
  - Reassemble TLS Application Data spanning multiple TLS records
  - Message Authentication Code (MAC), ignore "mac failed"
- Pre-Shared-Key:** An empty text input field.
- (Pre)-Master-Secret log filename:** A text input field containing the path '/Users/username/Documents/sslkeylog.log' and a 'Browse...' button to its right.

The Wireshark logo is visible in the top right corner of the interface.



# WEBPAGE ACQUISITION VIA BROWSER

---

- Open a new terminal window (#2) and run **"script w2.txt"** to store command line history in w2.txt file and place it in top right part of desktop
- Start video recording choosing the right resolution (let the output of all windows visible)

**apt-get install ffmpeg**

**ffmpeg -f x11grab -y -r 5 -s 1440x900 -i :0.0 -c:v libx264 video.avi**

- Good alternative: **OBS Studio**





# WEBPAGE ACQUISITION VIA BROWSER

---

- Open a new terminal window (#3), place it in bottom left part of desktop and run **"script w3.txt"** to store command line history in file w3.txt
- Start network traffic acquisition (let the output visible)

```
sudo tcpdump -n -U -s 65535 -w - | tee tcpdump.pcap | tcpdump -r -
```





# WEBPAGE ACQUISITION VIA BROWSER

---

- Focus on the terminal window #1 (top left) and move to "osdfcon2021" folder
- Run the following commands:

```
sudo ntpdate I.ro.pool.ntp.org | tee ntpdate.txt
```

```
cp /etc/hosts ./
```

```
traceroute www.osdfcon.org | dig traceroute.txt
```

```
dig www.osdfcon.org | tee dig.txt
```

```
whois osdfcon.org | tee whois.txt
```

```
13:43 .  
12:30 ..  
13:42 hosts  
13:41 sslkeylogfile.log  
13:41 strace.txt  
13:43 traceroute.txt  
13:41 traffic.pcap  
13:41 video.avi  
13:41 w1.txt  
13:41 w2.txt  
13:41 w3.txt  
13:43 whois.txt
```



# WEBPAGE ACQUISITION VIA BROWSER

---

- Stay focused on the terminal window #1 (top left)
- Start Chrome web browser with strace output running live on terminal

**`strace -r -f google-chrome-stable 2>&1 | tee strace.txt`**

- Place browser in bottom right area of desktop and navigate to your evidence



```
labimager@labimager: ~/osdfcon2021
labimager@labimager:~/osdfcon2021$ script w1.txt
Script started, output log file is 'w1.txt'.
labimager@labimager:~/osdfcon2021$ export SSLKEYLOGFILE="/home/labimager/osdfcon2021/sslkeylogfile.log"
labimager@labimager:~/osdfcon2021$ echo $SSLKEYLOGFILE
/home/labimager/osdfcon2021/sslkeylogfile.log
labimager@labimager:~/osdfcon2021$ strace -r -f google-chrome-stable 2>&1 | tee strace.txt

labimager@labimager:~/osdfcon2021
labimager@labimager:~/osdfcon2021$ script w2.txt
Script started, output log file is 'w2.txt'.
labimager@labimager:~/osdfcon2021$ ffmpeg -f x11grab -y -r 5 -s 1440x900 -i :0.0 -c:v libx264 video.avi

labimager@labimager:~/osdfcon2021
labimager@labimager:~/osdfcon2021$ cd osdfcon2021/
labimager@labimager:~/osdfcon2021$ script w3.txt
Script started, output log file is 'w3.txt'.
labimager@labimager:~/osdfcon2021$ sudo tcpdump -n -U -s 65535 -w - | tee traffic.pcap | tcpdump -r -
```



```
labimager@labimager: ~/osdfcon2021
File Actions Edit View Help

labimager@labimager: ~/osdfcon2021
[pid 5134] 0.000482 futex(0x7ffe1689ac90, FUTEX_WAIT_BITSET_PRIVATE, 0,
{tv_sec=9448, tv_nsec=478729996}, FUTEX_BITSET_MATCH_ANY) = -1 ETIMEDOUT (Co
nnection timed out)
[pid 5134] 0.052696 futex(0x7ffe1689ac40, FUTEX_WAKE_PRIVATE, 1) = 0
[pid 5134] 0.000510 futex(0x7ffe1689ac90, FUTEX_WAIT_BITSET_PRIVATE, 0,
{tv_sec=9448, tv_nsec=531971467}, FUTEX_BITSET_MATCH_ANY) = -1 ETIMEDOUT (Co
nnection timed out)
[pid 5134] 0.053457 futex(0x7ffe1689ac40, FUTEX_WAKE_PRIVATE, 1) = 0
[pid 5134] 0.000466 futex(0x7ffe1689ac90, FUTEX_WAIT_BITSET_PRIVATE, 0,
{tv_sec=9448, tv_nsec=585821977}, FUTEX_BITSET_MATCH_ANY)
```

```
labimager@labimager: ~/osdfcon2021
File Actions Edit View Help

labimager@labimager: ~/osdfcon2021
frame= 1136 fps=5.0 q=23.0 size= 16896kB time=00:03:36.80 bitrate= 638.4kbi
frame= 1139 fps=5.0 q=23.0 size= 16896kB time=00:03:37.40 bitrate= 636.7kbi
frame= 1142 fps=5.0 q=23.0 size= 16896kB time=00:03:38.00 bitrate= 634.9kbi
frame= 1145 fps=5.0 q=23.0 size= 16896kB time=00:03:38.60 bitrate= 633.2kbi
frame= 1148 fps=5.0 q=23.0 size= 16896kB time=00:03:39.20 bitrate= 631.4kbi
frame= 1151 fps=5.0 q=23.0 size= 16896kB time=00:03:39.80 bitrate= 629.7kbi
frame= 1154 fps=5.0 q=23.0 size= 17152kB time=00:03:40.40 bitrate= 637.5kbi
frame= 1157 fps=5.0 q=23.0 size= 17152kB time=00:03:41.00 bitrate= 635.8kbi
[s/s speed=0.957x
```

```
labimager@labimager: ~/osdfcon2021
File Actions Edit View Help

labimager@labimager: ~/osdfcon2021
12:45:08.945270 IP ml104s43-in-f3.1e100.net.443 > labimager.34148: UDP, lengt
h 25
12:45:13.135846 IP lhr35s10-in-f3.1e100.net.https > labimager.48984: Flags [F
P.], seq 4293, ack 582, win 64240, length 0
12:45:13.181326 IP labimager.48984 > lhr35s10-in-f3.1e100.net.https: Flags [.
.], ack 4294, win 62780, length 0
12:45:30.954646 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 5289, win 62780, length 0
12:45:31.886236 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 5972, win 62780, length 0
12:45:35.977805 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 6387, win 62780, length 0
12:45:35.978249 IP ml104s43-in-f3.1e100.net.https > labimager.48984: Flags [.
.], ack 1309, win 64240, length 0
12:45:36.157339 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 3705, win 62780, length 0
12:45:40.075147 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 23270, win 62780, length 0
12:45:40.075392 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 20673, win 62780, length 0
12:45:40.075517 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 5871, win 63986, length 0
12:45:40.075570 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 29400, win 62780, length 0
12:45:43.402082 IP labimager.48984 > ml104s43-in-f3.1e100.net.https: Flags [.
.], ack 635255, win 65535, length 0
```



## Forensic Acquisition of Websites, Webpages and Online Services with Open Source Tools



The slide displays a forensic analysis workflow. On the left, three terminal windows show network traffic capture and analysis. The top terminal shows a packet capture with details for a UDP message from 151.99.51.205. The middle terminal shows a list of captured UDP packets with their timestamps and lengths. The bottom terminal shows a list of captured UDP packets with their timestamps and lengths.

On the right, a terminal window shows video analysis statistics for a file named 'frame-14080'. The statistics include frame number, fps, q, size, time, and bitrate.

On the right side of the slide, a browser window shows a YouTube video player for the video 'OSDFCon'. The video player shows a thumbnail of a conference hall and the video title 'OSDFCon' by Tradotto. The video has 310 visualizzazioni and was uploaded on 23 ago 2016.

## Forensic Acquisition of Websites, Webpages and Online Services with Open Source Tools



# WEBPAGE ACQUISITION VIA BROWSER

---

- Some improvements:
  - You can take screenshots with Chrome Extensions
  - You can install **more extensions** to «certify» the navigation
  - You can **save webpages**
  - You can record **audio** (es. with OBS)
  - You can further filter through **mitmproxy** to show HTTP commands (and then route to destination)
  - You can download SSL certificates, Robots.txt, more DNS data



# WEBPAGE ACQUISITION VIA BROWSER

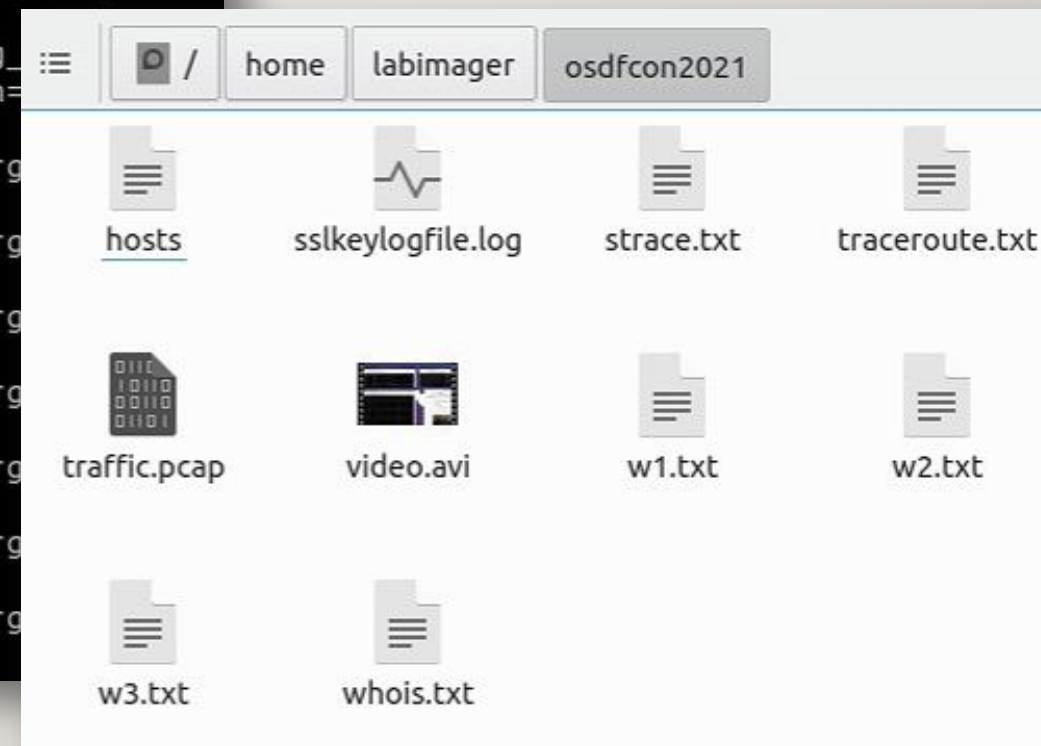
```
labimager@labimager:~/osdfcon2021$ tcpdump -r traffic.pcap | grep osdfcon
reading from file traffic.pcap, link-type EN10MB (Ethernet)
12:43:41.567755 IP labimager.44306 > _gateway.domain: 3044+ [1au] A? www.osdf
con.org. (44)
12:44:43.318621 IP labimager.46336 > _gateway.domain: 56484+ [1au] A?
fcon.org. (44)
12:46:16.949549 IP labimager.37309 > _gateway.domain: 60304+ [1au] A?
fcon.org. (44)
12:55:18.640826 IP labimager.56160 > _gateway.domain: 32196+ [1au] A?
fcon.org. (44)
12:58:25.982585 IP labimager.42771 > _gateway.domain: 48428+ [1au] A?
fcon.org. (44)
13:38:34.389186 IP labimager.56017 > _gateway.domain: 53788+ [1au] A?
fcon.org. (44)
```

```
labimager@labimager:~/osdfcon2021$ tcpdump -n -A -r traffic.pcap | grep 104.1
99.123.142 | head
reading from file traffic.pcap, link-type EN10MB (Ethernet)
12:43:41.886560 IP 192.168.140.2.53 > 192.168.140.128.44306: 3044 2/0/1 CNAME
basistech.wpengine.com., A 104.199.123.142 (96)
12:43:41.913105 IP 192.168.140.128.32918 > 104.199.123.142.443: Flags [S], se
q 345866730, win 64240, options [mss 1460,sackOK,TS val 3813182707 ecr 0,nop,
wscale 7], length 0
12:43:41.988515 IP 192.168.140.128.32920 > 104.199.123.142.443: Flags [S], se
q 3042072524, win 64240, options [mss 1460,sackOK,TS val 3813182782 ecr 0,nop
,wscale 7], length 0
12:43:42.089098 IP 104.199.123.142.443 > 192.168.140.128.32918: Flags [S.], s
eq 1327646689, ack 345866731, win 64240, options [mss 1460], length 0
12:43:42.089285 IP 192.168.140.128.32918 > 104.199.123.142.443: Flags [.], ac
k 1, win 64240, length 0
12:43:42.095281 IP 192.168.140.128.32918 > 104.199.123.142.443: Flags [P.], s
eq 1:518, ack 1, win 64240, length 517
12:43:42.095806 IP 104.199.123.142.443 > 192.168.140.128.32918: Flags [.], ac
k 518, win 64240, length 0
12:43:42.163247 IP 104.199.123.142.443 > 192.168.140.128.32920: Flags [S.], s
eq 404512752, ack 3042072525, win 64240, options [mss 1460], length 0
12:43:42.163332 IP 192.168.140.128.32920 > 104.199.123.142.443: Flags [.], ac
k 1, win 64240, length 0
12:43:42.174564 IP 192.168.140.128.32920 > 104.199.123.142.443: Flags [P.], s
eq 1:518, ack 1, win 64240, length 517
tcpdump: Unable to write output: Broken pipe
labimager@labimager:~/osdfcon2021$
```



# WEBPAGE ACQUISITION VIA BROWSER

```
labimager@labimager:~/osdfcon2021$ grep "osdfcon.org" strace.txt | head
[pid 4325] 0.000239 pwrite64(35, "1/0/_dk_https://osdfcon.org http"...
 130, 24 <unfinished ...>
[pid 4325] 0.000023 pwrite64(36, "1/0/_dk_https://osdfcon.org http"...
 115, 24 <unfinished ...>
[pid 4289] 0.000107 <... recvmsg resumed>{msg_name=NULL, msg_
msg_iov=[{iov_base="www.osdfcon.org/wp-content/uploa"... , iov_len=
g_iovlen=1, msg_controllen=0, msg_flags=0}, MSG_DONTWAIT) = 1024
[pid 4325] 0.000021 pwrite64(37, "1/0/_dk_https://osdfcon.org
 203, 24 <unfinished ...>
[pid 4325] 0.000092 pwrite64(39, "1/0/_dk_https://osdfcon.org
 115, 24 <unfinished ...>
[pid 4338] 0.000026 pwrite64(42, "1/0/_dk_https://osdfcon.org
 117, 24 <unfinished ...>
[pid 4322] 0.000057 pwrite64(36, "1/0/_dk_https://osdfcon.org
 203, 24 <unfinished ...>
[pid 4338] 0.000036 pwrite64(39, "1/0/_dk_https://osdfcon.org
 117, 24 <unfinished ...>
[pid 4338] 0.000042 pwrite64(40, "1/0/_dk_https://osdfcon.org
 125, 24 <unfinished ...>
[pid 4322] 0.000034 pwrite64(47, "1/0/_dk_https://osdfcon.org
 123, 24 <unfinished ...>
```







# WEBPAGE ACQUISITION VIA BROWSER

---

- Close browser, stop tcpdump, stop ffmpeg/obs
- Save “script” history with **CRTL+D**
- `tar -czvf acquisition.tar.gz`
- `/home/labimager/.local/bin/ots stamp acquisition.tar.gz`
- Close virtual machine
- Zip whole VM folder
- Apply timestamp to zipped VM



# WEBPAGE ACQUISITION VIA BROWSER

The screenshot displays a desktop environment with four windows:

- Terminal 1 (top-left):** Shows network connection logs. Key lines include:

```
connection timed out
[pid 5287] 0.006182 futex(0x7ffe1689ac40, FUTEX_WAKE_PRIVATE, 1) = 0
[pid 5287] 0.000910 lseek(26, 0, SEEK_SET) = 0
[pid 5287] 0.001418 read(26, "7443089 66220 34076 35132 0 8084"... , 4095) = 36
[pid 5287] 0.000807 lseek(27, 0, SEEK_SET) = 0
[pid 5287] 0.000618 read(27, "Name:\tchrome\nUmask:\t0002\nState:\t"... , 4095) = 1428
[pid 5287] 0.000596 futex(0x7ffe1689ac90, FUTEX_WAIT_BITSET_PRIVATE, 0, {tv_sec=10151, tv_nsec=981971908}, FUTEX_BITSET_MATCH_ANY)
```
- Terminal 2 (top-right):** Shows video acquisition statistics:

```
frame= 1238 fps=5.0 q=23.0 size= 15104kB time=00:03:57.20 bitrate= 521.6kbi
frame= 1241 fps=5.0 q=23.0 size= 15104kB time=00:03:57.80 bitrate= 520.3kbi
frame= 1244 fps=5.0 q=23.0 size= 15104kB time=00:03:58.40 bitrate= 519.0kbi
frame= 1247 fps=5.0 q=23.0 size= 15104kB time=00:03:59.00 bitrate= 517.7kbi
frame= 1250 fps=5.0 q=23.0 size= 15104kB time=00:03:59.60 bitrate= 516.4kbi
frame= 1253 fps=5.0 q=23.0 size= 15104kB time=00:04:00.20 bitrate= 515.1kbi
frame= 1256 fps=5.0 q=23.0 size= 15104kB time=00:04:00.80 bitrate= 513.8kbi
frame= 1259 fps=5.0 q=23.0 size= 15104kB time=00:04:01.40 bitrate= 512.6kbi
@s/s speed=0.96x
```
- Terminal 3 (bottom-left):** Shows a list of network connections:

```
12:57:11.252264 IP zrh04s14-in-f14.1e100.net.443 > labimager.56358: UDP, length 100
12:57:11.252311 IP zrh04s14-in-f14.1e100.net.443 > labimager.56358: UDP, length 95
12:57:11.254947 IP labimager.56358 > zrh04s14-in-f14.1e100.net.443: UDP, length 36
12:57:11.274780 IP zrh04s14-in-f14.1e100.net.443 > labimager.56358: UDP, length 26
12:57:11.281569 IP labimager.56358 > zrh04s14-in-f14.1e100.net.443: UDP, length 33
12:57:12.298553 IP labimager.42842 > 104.17.131.171.https: Flags [.], ack 1730, win 64028, length 0
12:57:12.298957 IP 104.17.131.171.https > labimager.42842: Flags [.], ack 1354, win 64240, length 0
12:57:14.350961 IP labimager.32846 > 104.18.20.191.https: Flags [.], ack 2034, win 64028, length 0
12:57:14.351267 IP 104.18.20.191.https > labimager.32846: Flags [.], ack 1263, win 64240, length 0
12:57:14.433831 IP labimager.46048 > ml04s25-in-f10.1e100.net.https: Flags [.], ack 7233, win 62780, length 0
12:57:16.398728 IP labimager.45440 > 144.2.12.5.https: Flags [.], ack 3956, win 62780, length 0
12:57:16.399184 IP 144.2.12.5.https > labimager.45440: Flags [.], ack 1873, win 64240, length 0
12:57:23.113278 IP labimager.51044 > ml04s43-in-f6.1e100.net.https: Flags [.], ack 5142, win 62780, length 0
```
- Browser (bottom-right):** Shows a YouTube search result for 'osdfcon'. The search results include:
  - OSDFCon 2020** by Basis Technology: "Putting Together the RDPiece, Brian Moran, OSDFCon 2020 • 84:30" and "Using Past Data to Determine Relevance in Autopsy, Brian Carrier, ... • 29:16".
  - OSDFCon**: "310 visualizzazioni • 5 anni fa" by Basis Technology. Description: "Unisciti ad altri investigatori e sviluppatore il 26 ottobre 2016 per la 7a Conferenza annuale Open Source Digital Forensics ...".



# RECURSIVE ACQUISITION OF WEBSITES

---

- Install wget with SSLKEYLOG compatibility (must use libgnutls):

```
sudo apt install build-essential pkg-config libgnutls28-dev nettle-bin nettle-dev
wget https://ftp.gnu.org/gnu/wget/wget-1.20.3.tar.gz
sudo apt remove wget
tar -xvf wget-1.20.3.tar.gz
cd wget-1.20.3/
./configure --prefix=/usr --sysconfdir=/etc
make
sudo make install
```



# RECURSIVE ACQUISITION OF WEBSITES

---

- The process is similar to the forensic acquisition of webpages
- Instead of launching the browser, simply launch

```
strace -r -f wget -m --keep-session-cookies --save-cookies=cookies.txt --limit-  
rate=500k -w I --random-wait --no-check-certificate -e robots=off -o log.txt -vv  
-S --preserve-permissions -np -E -k -K -p --show-progress  
https://www.osdfcon.org 2>&I | tee strace.txt
```



# RECURSIVE ACQUISITION OF WEBSITES

---

- Remember that wget does not download SSL certificate and robots

```
wget https://www.osdfcon.org/robots.txt -P robots.txt --no-check-certificate -o  
wget_log_robots.txt
```

```
openssl s_client -connect www.osdfcon.org:443 > ssl.txt
```



# WEBPAGE ACQUISITION VIA BROWSER

---

- Upon wget completion, stop tcpdump, stop ffmpeg/obs
- `tar -czvf acquisition.tar.gz`
- `/home/labimager/.local/bin/ots stamp acquisition.tar.gz`
- Close virtual machine
- Zip whole VM folder
- Apply timestamp to zipped VM



## FURTHER IMPROVEMENTS

---

- Install in the VM several **tools to acquire/attest their online evidences**:
  - Google Earth
  - Torrent
  - Android Emulator (Instant Messaging, etc...)
  - Other Operating Systems (Windows guest, etc...)
  - Other VM (Android VM such as "Nox», "Genymotion" or "AVD)
  - More tools...
- More **tricks** can be needed (sniffing and decrypting network traffic, etc...)
- Run **VPN/Tor** to exit from differen Countries or from Tor exit nodes (set sock5 proxy)
- Many others...



## CONCLUSIONS AND FUTURE WORK

---

- That's only the basics, much more can be done also to avoid possible tampering
- Write script for automatic Forensic Acquisition of Websites
  - Sslkeylog + video + tcpdump/mitmproxy + wget + strace + script + zip + ots
- Write script to launch Web Browser for quick Acquisition of Webpages
  - Sslkeylog + video + tcpdump/mitmproxy + chrome/firefox + strace + script + zip + ots
- Use PhantomJS to automate acquisition of webpages or websites





# THANKS

---

Thanks for watching!