Report of Claire Fei *(z5161105)*

Nitroba University Case
5th Nov 2019

Contents

Preliminary

1) I am Claire Fei whose address is 123 real street, Sydney, in the State of New South Wales.
2) I have graduated from an Australian High School in New South Wales and have gained a Higher School Certificate (HSC).
3) I am in my third and final year of studying at the University of New South Wales, Sydney, currently undertaking a Bachelor of Science (Computer Science) with a major in Computer Security.
4) I am currently undertaking a course run by Ajoy Ghosh called Digital Forensics (course code COMP6445) whom has taught postgraduate law, engineering and information technology students in various Australian and international universities and is a Certified Professional (CP) by the Australian Computer Society.
5) I have taken many other courses of interest including Extended Security Engineering and Cyber Security, Security Assessment (COMP6441) and Web Application and Security (COMP6443).
6) I am currently working at an EduTech company called School Bytes as a Full Stack Developer.

Instructions and Scope of this report

1) A teacher in the Chemistry Department, Lily Tuckrige (Tuckrige), claims to be receiving harassing emails, suspected to be coming from her Chemistry 109 class in which she is teaching this Summer.
2) Evidence of these emails, send to her personal account lilytuckrige@yahoo.com has been received by the system administrator, along with header information revealing an IP originating from a Nitroba share-room with a public wifi.
3) Nitroba has placed a network snigger on the ethernet port and hence all network traffic and packets are logged.
4) I have been instructed to undertake technical analysis of the results of the network sniffing to determine if one of the students in the class was responsible for the harassing email and if so, which of the students are responsible.
5) My technical analysis must discover the email's sender and in the process, create contemporaneous notes and record any data files.
6) I must demonstrate the reliability of my conclusion by showing an alternate solution/ tools to arrive at the same result.

Summary of Findings and Opinions

1) The offender had a search history containing incriminating evidence relevant to the case including "i want to harass my teacher".
2) On the same device, and at a similar time to this search, the willselfdestruct website was accessed the day before Lily Tuckrige received the offending email.
3) On the same device, and at a similar time, the gmail account "jcoach@gmail.com" was accessed.

4) Based on the balance of probabilities, containing the evidence above, and the probability that only Johnny Coach has access to his email account "jcoach@gmail.com", Johnny Coach is the sender of the harassing email to Lily Tuckrige.

Body of Report

1) After receiving the forensic copy, the first step is to create and verify the hash of the copy. This can be done by creating an MD5 hash of the file by running the command shown below.

```
Claires-MacBook-Pro:Downloads claire.fei$ md5sum nitroba.pcap
9981827f11968773ff815e39f5458ec8  nitroba.pcap
```

The md5 algorithm creates a "digital fingerprint" by converting the data from a "larger" file into a shorter string. Hence, if the data in the file is unchanged, the same string should be produced if the same md5 algorithm is run across the data thus allowing us to verify the integrity of the file.

First Solution - Provided Solution

2) The first step in analysing the provided ".pcap" file is to use tcpflow to create the network flow. The provided pcap file is a representation of all network exchanged and the data stored in a file. We use the command "tcpflow -r nitroba.pcap -o nitroba-netflows" to direct the network analysis done by the program tcpflow into a directory (folder).

```
root@kali:~/Documents/nitroba# tcpflow -r nitroba.pcap -o nitroba-netflows/
reportfilename: nitroba-netflows//report.xml
```

3) Next, we want to navigate into the folder by using the command "cd nitroba-netflow". We will use the tool grep to assist us with finding data more quickly. Grep is a way for a user to do a basic text search and is the equivalent of user typing something into the search bar in Google to narrow down results.

```
root@kali:~/Documents/nitroba# cd nitroba-netflows/
root@kali:~/Documents/nitroba/nitroba-netflows# grep -l "will self destruct" *
069.025.094.022.00080-192.168.015.004.35984
069.025.094.022.00080-192.168.015.004.35984c1
069.025.094.022.00080-192.168.015.004.36046
069.025.094.022.00080-192.168.015.004.36046c1
```

The result of using the grep command is that it will "streams". These data streams are a sequence of signals transmitted and received by devices in order to transmit information/data.

4) Since these streams were the ones that contained the text "will self destruct", they will most likely contain interesting information. As such, we will want to view what is contained within these streams by using the command "cat". The cat command allows us to view the contents of a file. Notice that the words "anonymous email" are all common among all three streams.

```
root@kali:~/Documents/nitroba/nitroba-netflows# cat 069.025.094.022.00080-192.168.015.004.35984
HTTP/1.1 200 OK
Date: Tue, 22 Jul 2008 07:24:05 GMT
Server: Apache
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: JSESSIONID=0FB2AD5FEEF73F78A1D0A5492813C761; Path=/
Content-Type: text/html;charset=ISO-8859-1
Connection: close
Transfer-Encoding: chunked

1ff8


<html>
<head>
    <meta name="Description" content="Secure, anonymous email and messaging for sensitive data.  Send a self-de
structing email to a friend, client or colleague." />
    <meta name="KeyWords" content="secure anonymous self destruct email message page, will self destruct email
message, secret secure anonymous email message," />
    <title>FREE secure anonymous E-mail to a friend, client or colleague: WillSelfDestruct</title>
</head>
```

```
root@kali:~/Documents/nitroba/nitroba-netflows# cat 069.025.094.022.00080-192.168.015.004.36046
HTTP/1.1 200 OK
Date: Tue, 22 Jul 2008 07:24:45 GMT
Server: Apache
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: JSESSIONID=C0AC3EC4944A8C88D98B7A8020B12492; Path=/
Content-Type: text/html;charset=ISO-8859-1
Connection: close
Transfer-Encoding: chunked

1ff8

<html>
<head>
    <meta name="Description" content="Secure, anonymous email and messaging for sensitive data.  Send a self-de
structing email to a friend, client or colleague." />
    <meta name="KeyWords" content="secure anonymous self destruct email message page, will self destruct email
message, secret secure anonymous email message," />
    <title>FREE secure anonymous E-mail to a friend, client or colleague: WillSelfDestruct</title>
</head>
<body>
<center>
    <style media="print"  type="text/css">
        #body {
            display: none;
        }
    </style>
```

```
root@kali:~/Documents/nitroba/nitroba-netflows# cat 069.025.094.022.00080-192.168.015.004.36046c1
HTTP/1.1 200 OK
Date: Tue, 22 Jul 2008 07:24:45 GMT
Server: Apache
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: JSESSIONID=C0AC3EC4944A8C88D98B7A8020B12492; Path=/
Content-Type: text/html;charset=ISO-8859-1
Connection: close
Transfer-Encoding: chunked

1ff8

<html>
<head>
    <meta name="Description" content="Secure, anonymous email and messaging for sensitive data.  Send a self-de
structing email to a friend, client or colleague." />
    <meta name="KeyWords" content="secure anonymous self destruct email message page, will self destruct email
message, secret secure anonymous email message," />
    <title>FREE secure anonymous E-mail to a friend, client or colleague: WillSelfDestruct</title>
</head>
<body>
<center>
    <style media="print"  type="text/css">
        #body {
```

5) Hence, we will want to use the grep tool again to search for streams of transmitted data containing the words “anonymous email” in order to find more relevant evidence. Notice that there is only one new and different result from the previous grep search.

```
root@kali:~/Documents/nitroba/nitroba-netflows# grep -l "anonymous email" *
069.025.094.022.00080-192.168.015.004.35984
069.025.094.022.00080-192.168.015.004.35984c1
069.025.094.022.00080-192.168.015.004.36046
069.025.094.022.00080-192.168.015.004.36046c1
069.080.225.091.00080-192.168.015.004.35848
069.080.225.091.00080-192.168.015.004.35848c1
```

6) We will now investigate this newly identified stream of data by using the cat command again to view the contents in text form. One interesting thing noticed in the contents of this stream is the email with the address “sendanonymousemail”

```
root@kali:~/Documents/nitroba/nitroba-netflows# cat 069.080.225.091.00080-192.168.015.004.35848
HTTP/1.1 200 OK
Date: Tue, 22 Jul 2008 07:21:37 GMT
Server: Apache/1.3.37 (Unix) PHP/4.4.4 with Suhosin-Patch
X-Powered-By: PHP/4.4.4
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

d9c
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
<title>Send Anonymous Email</title>
<link href="style.css" rel="stylesheet" type="text/css">

<script type="text/JavaScript">
<!--
function MM_findObj(n, d) { //v4.01
  var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
    d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
  if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
  for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
  if(!x && d.getElementById) x=d.getElementById(n); return x;
}
```

```
                                    <strong>
                                    Your IP Address is 70.134.91.12
                                    so don't do anything illegal.</strong>                    <strong>I
f you send death threats, abuse, slander or anything illegal we WILL publish your IP address and block you from
 this site.</strong> <br>
                                    <br>
                                    Abusers can be reported <a href="mailto:sendanonymousemail@gmail.com"
>here</a>.<br>
                    <br>
                    Please read our <A href="terms.php" target="_blank">terms
                  of use</A>.
                  <td width="54%" valign="top"><form action="send.php" method="post">
                    <table width="350" height="260" align="center" cellpadding=0 cellspacing=3 bgcolor="#EFEF
EF">
                      <tr valign=top>
                        <td align=center nowrap><span class="middle"><strong>Send
                              Anonymous Email </strong><br>
```

7) We will further search for evidence by using the email address we found as the new text to search for within the network streams.

```
root@kali:~/Documents/nitroba/nitroba-netflows# grep -l "sendanonymousemail" *
069.080.225.091.00080-192.168.015.004.35848
069.080.225.091.00080-192.168.015.004.35848c1
069.080.225.091.00080-192.168.015.004.35876
069.080.225.091.00080-192.168.015.004.35876c1
192.168.015.004.35798-074.125.019.104.00080
192.168.015.004.35798-074.125.019.104.00080c1
192.168.015.004.35848-069.080.225.091.00080
192.168.015.004.35848-069.080.225.091.00080c1
192.168.015.004.35850-069.080.225.091.00080
192.168.015.004.35850-069.080.225.091.00080c1
192.168.015.004.35852-074.125.019.167.00080
192.168.015.004.35852-074.125.019.167.00080c1
192.168.015.004.35854-074.125.019.167.00080
192.168.015.004.35854-074.125.019.167.00080c1
192.168.015.004.35856-067.015.076.053.00080
192.168.015.004.35856-067.015.076.053.00080c1
192.168.015.004.35876-069.080.225.091.00080
192.168.015.004.35876-069.080.225.091.00080c1
192.168.015.004.35878-074.125.019.167.00080
192.168.015.004.35878-074.125.019.167.00080c1
192.168.015.004.35880-074.125.019.167.00080
192.168.015.004.35880-074.125.019.167.00080c1
192.168.015.004.35882-067.015.076.053.00080
192.168.015.004.35882-067.015.076.053.00080c1
192.168.015.004.35886-067.015.076.053.00080
192.168.015.004.35886-067.015.076.053.00080c1
```

8) Using the cat command on each of these will show you the contents of data transmitted in each of the network streams. The one that we took particular notice of is the stream “192.168.015.004.35876-069.080.225.091.00080”. We can clearly see that this is the stream that transmitted the data for the harassing email, as indicated by the contents circled in red below containing the message “your class stinks” etc.

```
root@kali:~/Documents/nitroba/nitroba-netflows# cat 192.168.015.004.35876-069.080.225.091.00080
POST /send.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.sendanonymousemail.net/
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.sendanonymousemail.net
Content-Length: 275
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa

email=lilytuckrige@yahoo.com&sender=the_whole_world_is_watching@nitroba.org&subject=Your+class+stinks&message=W
hy+do+you+persist+in+teaching+a+boring+class%3F%0D%0A%0D%0AWe+don%27t+like+it.%0D%0A%0D%0AWe+don%27t+like+you.%
0D%0A%0D%0A&security_code=xkpmkb&submit=+++SEND%21+++GET /CaptchaSecurityImages.php?width=100&height=40&charact
er=5 HTTP/1.1
Accept: */*
Referer: http://www.sendanonymousemail.net/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.sendanonymousemail.net
Connection: Keep-Alive
Cookie: PHPSESSID=762adba03236142ccec305f6a20aaffa
```

9) From the name of the stream (the first few blocks of numbers), we know that the IP address “192.168.015.004” is a suspicious and interesting place to look. An IP address is a numerical label of each device connected to a network and hence may help us identify the suspicious device and hence user. We can narrow down the search by checking User-Agents of data transmissions that have interacted with this IP address. User-Agents are a way of identifying the operating system and browser of a user to the web server from which they are requesting information. We can use the grep search tool to find the User-Agents of the stream that we were looking at in step 8.

```
root@kali:~/Documents/nitroba/nitroba-netflows# grep -a User-Agent 192.168.015.004.35876-069.080.225.091.00080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

10) Using the results from above, we can see that the user agents are the same, suggesting the same software (e.g browser - internet explorer 6.0) and device was used. Hence we can do a reverse search to see if we can find all the streams where the device and software is consistent - since the perpetrator may change locations hence changing their IP address (numerical label to their device assigned by the network). Notice that on the right hand side of the command we specify “> user-agent-list”. This tells the command to place it’s output into a file called “user-agent-list”.

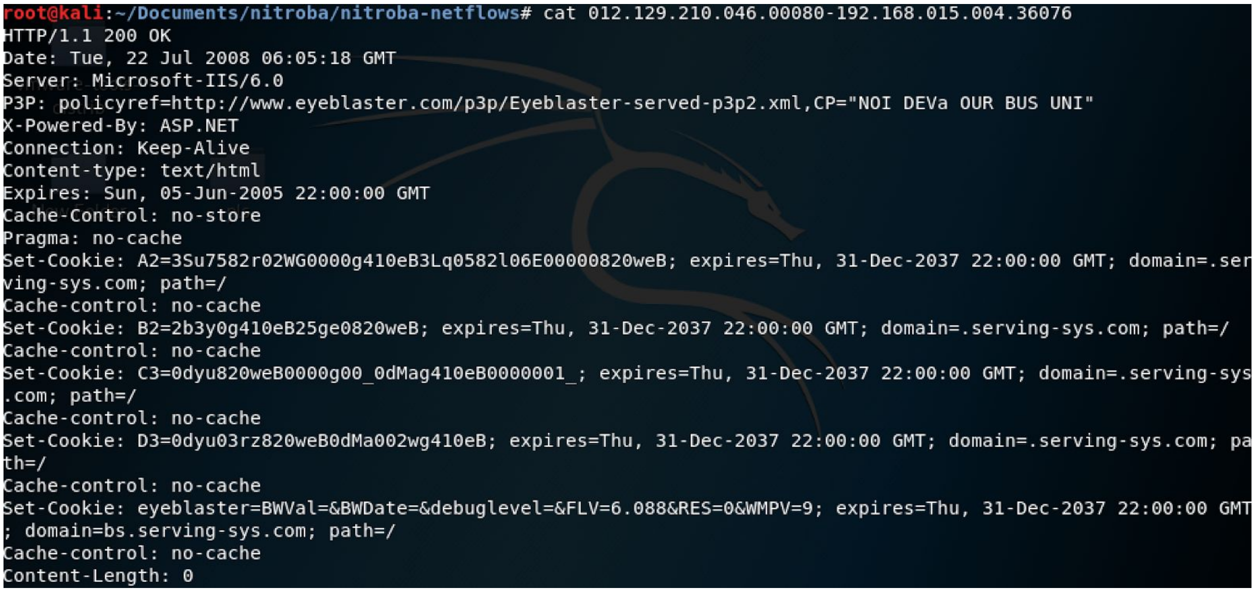
```
root@kali:~/Documents/nitroba/nitroba-netflows# grep -l 'Mozilla/4.0 .compatible; MSIE 6.0; Windows NT 5.1; SV1
.' * > user-agent-list
```

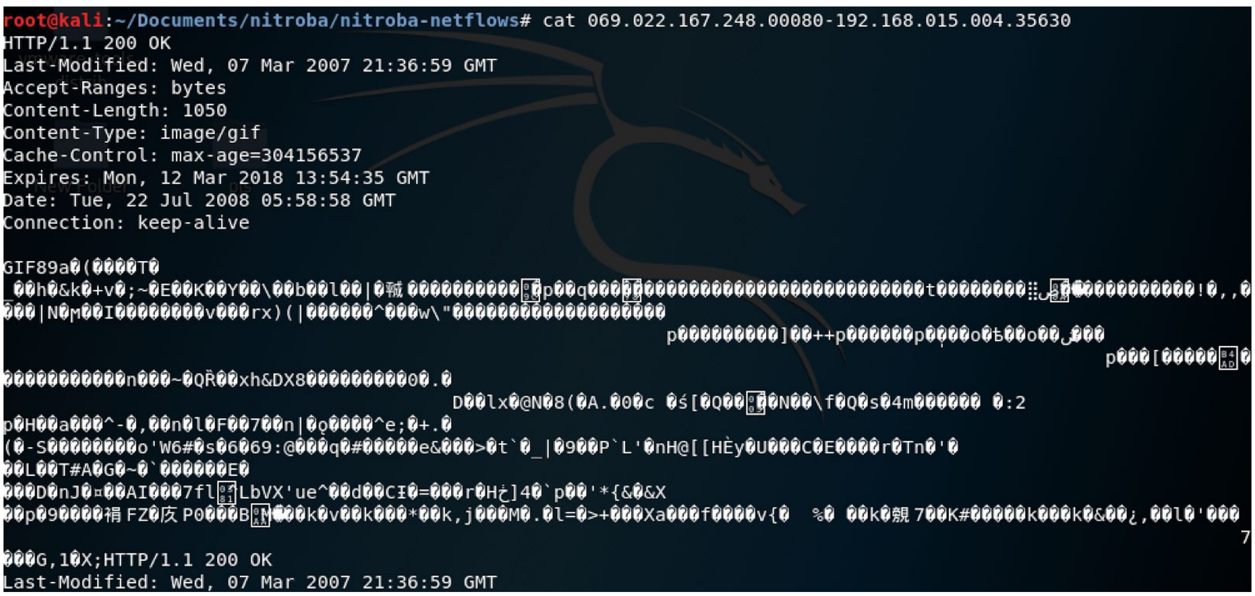
11) The next step is crucial in figuring out who the attacker is. Currently we are only getting the message that the browser sends to the web server (i.e the html we saw), however, we actually want the response. In order to find the matching response for each of the streams, we want to swap the source and destination around. Currently, we have it in the format of (source_ip-destination_ip). To swap it around and hence find the response streams, we can execute the command below.

```
root@kali:~/Documents/nitroba/nitroba-netflows# awk -F- '{print $2, "-", $1}' user-agent-list | sed 's/ //g' >
user-agent-rev
```

The results will now be stored in a file called “user-agent-rev”

12) Now that we have a list of the responses, we can use the cat command to view the contents of each of the streams. Notice that a lot of these files contain random information that either may not be interpreted, or does not seem relevant to the investigation.


root@kali:~/Documents/nitroba/nitroba-netflows# cat 012.129.210.046.00080-192.168.015.004.36076
HTTP/1.1 200 OK
Date: Tue, 22 Jul 2008 06:05:18 GMT
Server: Microsoft-IIS/6.0
P3P: policyref=http://www.eyeblaster.com/p3p/Eyeblaster-served-p3p2.xml,CP="NOI DEVa OUR BUS UNI"
X-Powered-By: ASP.NET
Connection: Keep-Alive
Content-type: text/html
Expires: Sun, 05-Jun-2005 22:00:00 GMT
Cache-Control: no-store
Pragma: no-cache
Set-Cookie: A2=3Su7582r02WG0000g410eB3Lq0582l06E00000820weB; expires=Thu, 31-Dec-2037 22:00:00 GMT; domain=.serving-sys.com; path=/
Cache-control: no-cache
Set-Cookie: B2=2b3y0g410eB25ge0820weB; expires=Thu, 31-Dec-2037 22:00:00 GMT; domain=.serving-sys.com; path=/
Cache-control: no-cache
Set-Cookie: C3=0dyu820weB0000g00_0dMag410eB0000001_; expires=Thu, 31-Dec-2037 22:00:00 GMT; domain=.serving-sys.com; path=/
Cache-control: no-cache
Set-Cookie: D3=0dyu03rz820weB0dMa002wg410eB; expires=Thu, 31-Dec-2037 22:00:00 GMT; domain=.serving-sys.com; path=/
Cache-control: no-cache
Set-Cookie: eyeblaster=BWVal=&BWDate=&debuglevel=&FLV=6.088&RES=0&WMPV=9; expires=Thu, 31-Dec-2037 22:00:00 GMT; domain=bs.serving-sys.com; path=/
Cache-control: no-cache
Content-Length: 0


root@kali:~/Documents/nitroba/nitroba-netflows# cat 069.022.167.248.00080-192.168.015.004.35630
HTTP/1.1 200 OK
Last-Modified: Wed, 07 Mar 2007 21:36:59 GMT
Accept-Ranges: bytes
Content-Length: 1050
Content-Type: image/gif
Cache-Control: max-age=304156537
Expires: Mon, 12 Mar 2018 13:54:35 GMT
Date: Tue, 22 Jul 2008 05:58:58 GMT
Connection: keep-alive
HTTP/1.1 200 OK
Last-Modified: Wed, 07 Mar 2007 21:36:59 GMT

After viewing all these streams, we notice that there are two in particular that contain suspicious and convicting information, namely “074.125.019.104.00080-192.168.015.004.35796” and “074.125.019.104.00080-192.168.015.004.35798” which contain the email address of a student.

```
root@kali:~/Documents/nitroba/nitroba-netflows# cat 074.125.019.104.00080-192.168.015.004.35796 | head -n 20
HTTP/1.1 302 Moved Temporarily
Set-Cookie: CAL=DQAAAG4AAAAyprUKisFp1wFlwiwIIZowqnpAerq-KS7yto_wd6bxSPzzEXHl0StDzuPdNyyn__poTb_5cy6Oflk7HqznK3Q
MZyVK0v0dzSPDiLSkyWSL0U2yIpYhnj94aV1D-RTdxjidUFLs32SWCI7EULqR4cD0;Domain=www.google.com;Path=/calendar;Expires=
Wed, 06-Aug-2008 06:01:08 GMT
Location: http://www.google.com/calendar/render?utm_campaign=en&utm_source=en-ha-na-us-bk&utm_medium=ha&utm_ter
m=google+calendar
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Date: Tue, 22 Jul 2008 06:01:08 GMT
Expires: Tue, 22 Jul 2008 06:01:08 GMT
Cache-Control: private, max-age=0
Content-Length: 237
Server: GFE/1.3

mP@J@0@@+B/@F@@T@n@
]                 @7%g!@@wq@@@@@@@k@@w@T@@@@@6@@@@w-@w@z+@@
?@eF@@@G@/@@*@@qru@y@@                                    @i@V@9@@@@@=!@@@@@@@H1@@#.@@@@@z@`@@@>l@b@@@\@@,@@@
E@UA3%.@@@@@@@@
PR@E
    @%NH@/[D8HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: secid=708511d04431b1dbce35563e903f2854; Path=/calendar
Set-Cookie: OL_SESSION=jcoachj@gmail.com-cal
```

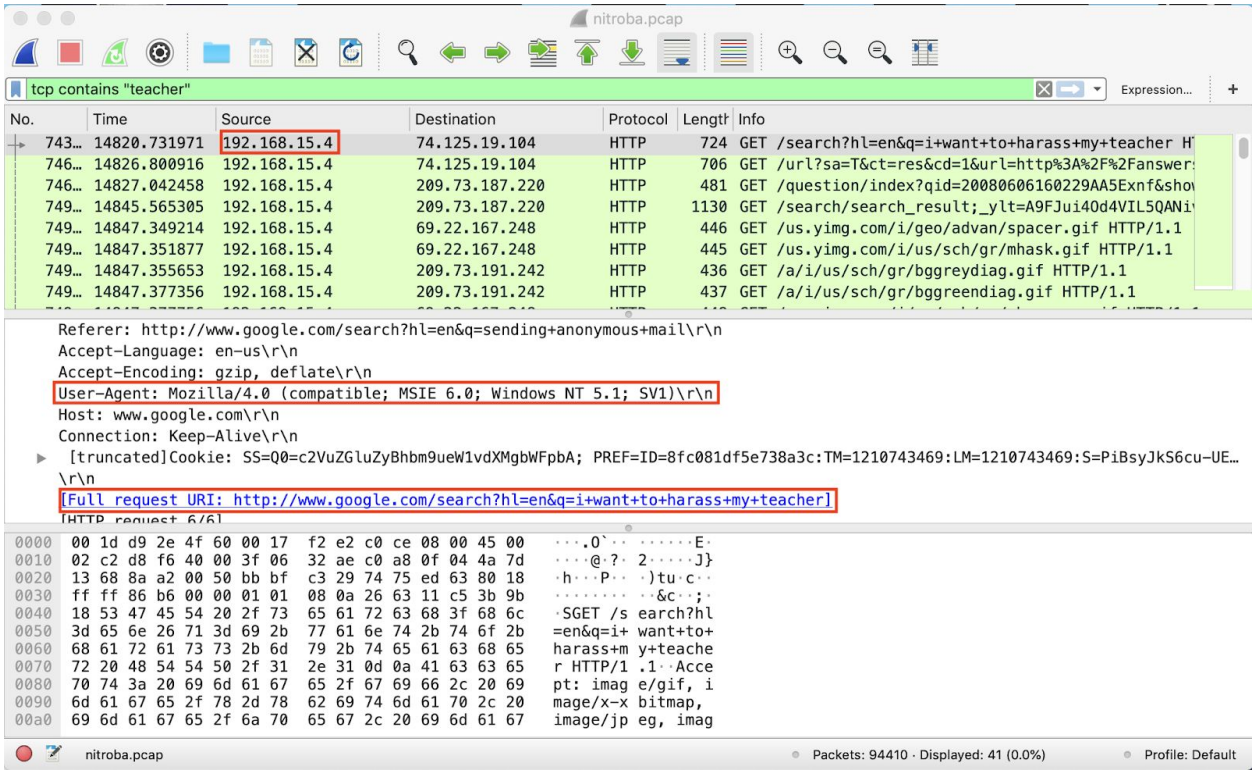
13) The files found in step 12 indicate that a user has logged in via gmail and since gmail requires a password, based on the balance of probabilities that the person who knows the password is the one logged in and hence constructed the crime, we can suspect that the perpetrator is Johnny Coach (Coach) since the email is aliased under his name "jcoachj@gmail.com". We can do a grep text search on this email to find other services that Coach has accessed whilst logged in to his email.

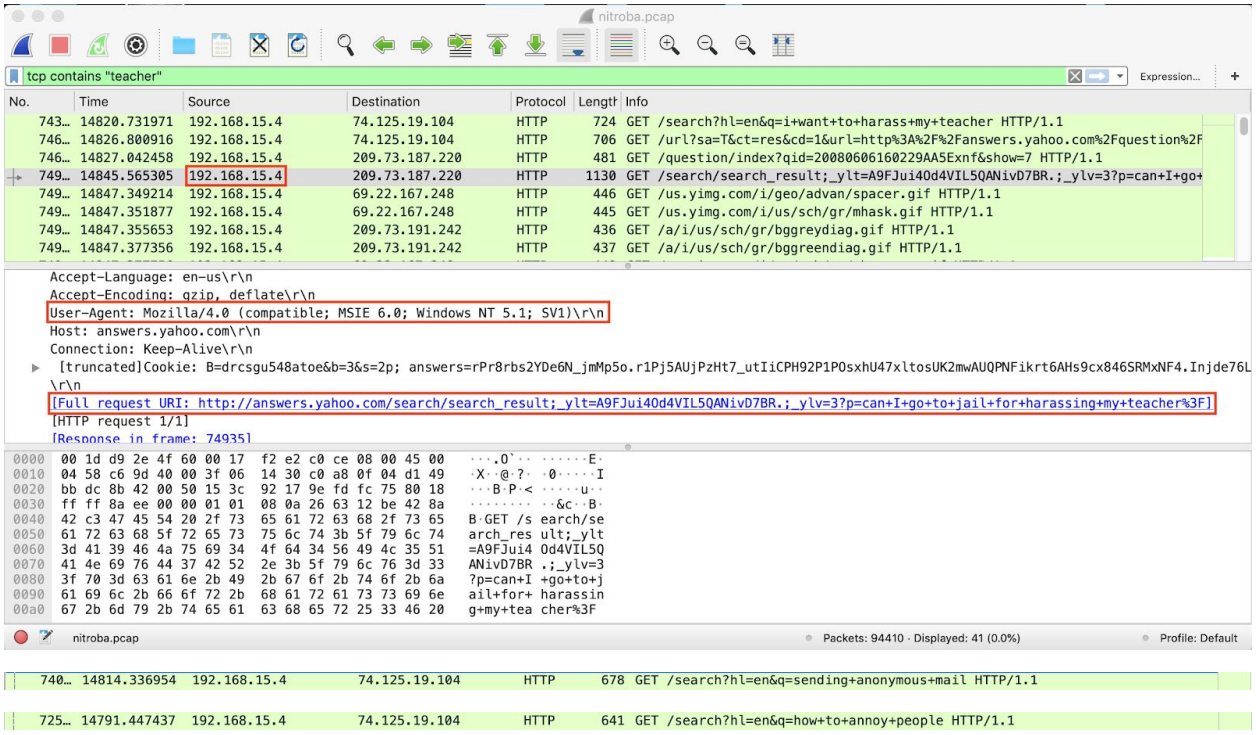
```
root@kali:~/Documents/nitroba/nitroba-netflows# grep -l jcoachj@gmail.com *
074.125.019.104.00080-192.168.015.004.35796
074.125.019.104.00080-192.168.015.004.35796c1
074.125.019.104.00080-192.168.015.004.35798
074.125.019.104.00080-192.168.015.004.35798c1
192.168.015.004.35796-074.125.019.104.00080
192.168.015.004.35796-074.125.019.104.00080c1
192.168.015.004.35798-074.125.019.104.00080
192.168.015.004.35798-074.125.019.104.00080c1
192.168.015.004.35804-074.125.019.017.00080
192.168.015.004.35804-074.125.019.017.00080c1
192.168.015.004.35824-074.125.019.017.00080
192.168.015.004.35824-074.125.019.017.00080c1
192.168.015.004.35826-209.085.201.189.00080
192.168.015.004.35826-209.085.201.189.00080c1
192.168.015.004.35828-209.085.201.189.00080
192.168.015.004.35828-209.085.201.189.00080c1
192.168.015.004.35832-074.125.019.017.00080
192.168.015.004.35832-074.125.019.017.00080c1
192.168.015.004.35834-074.125.019.017.00080
192.168.015.004.35834-074.125.019.017.00080c1
192.168.015.004.35846-074.125.019.104.00080
192.168.015.004.35846-074.125.019.104.00080c1
```

14) Hence the conclusion is that Coach was the one that send the offending and harassing emails.

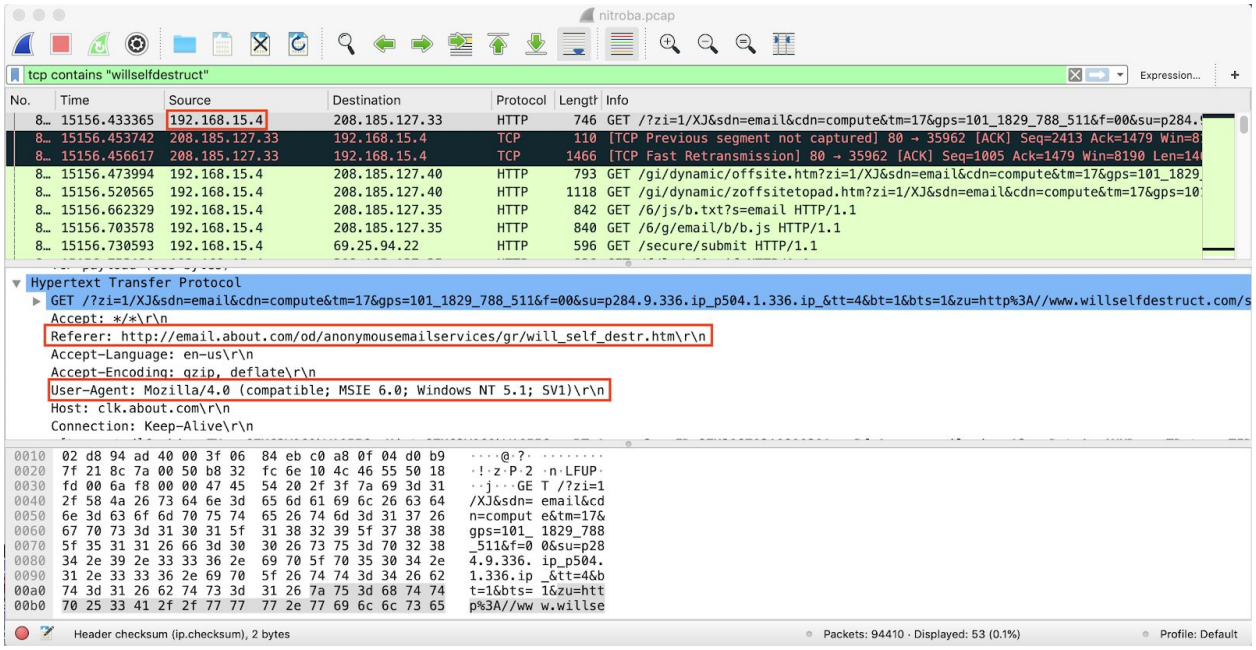
Alternate Solution - Wireshark (for reliability)

2) Firstly, using “tcp contains <keyword>” which acts as a search functionality for web requests containing keywords, I searched for keywords such as teacher. Then looking at each web requests, it is clear that a user was searching for information on the internet such as “I want to harass my teacher”,“I go to jail for harassing my teacher”, “how to annoy people” and “send anonymous email”. Notice that both of these are originating from the same IP address (numerical label of each device connected to a network and hence identity) and has the same User-Agent which allows you to identify the device. In this case, it seems the user searching for harassment methods and consequences was on a Windows computer using internet explorer 6.0.



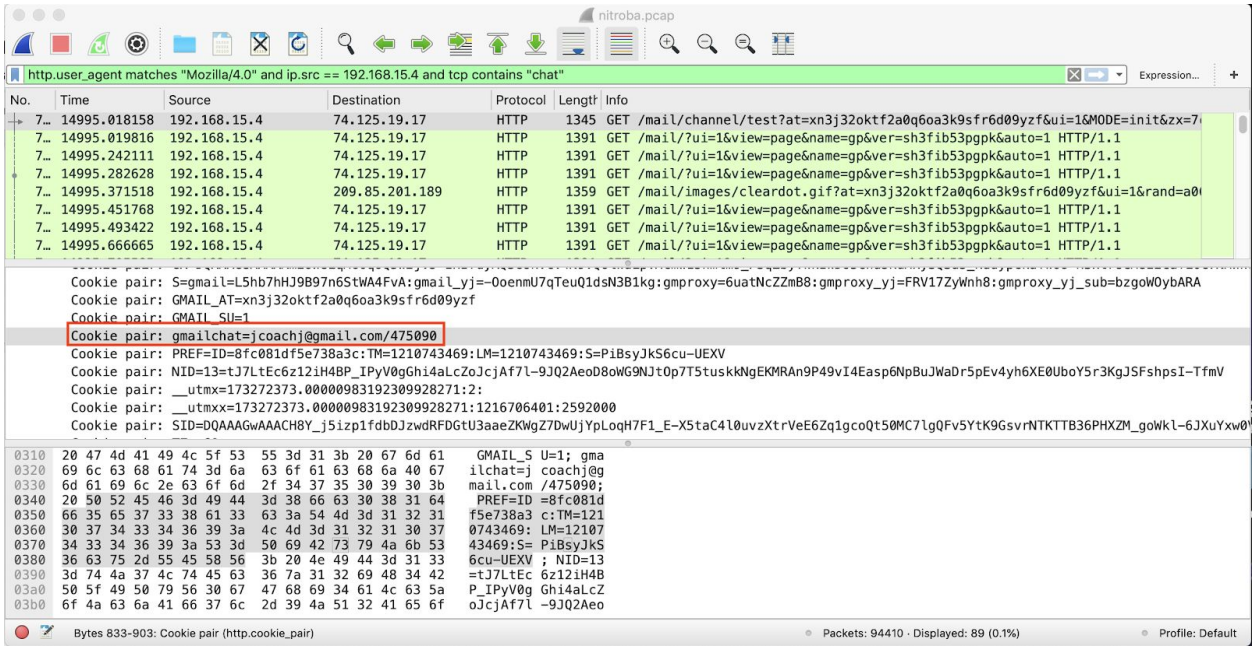


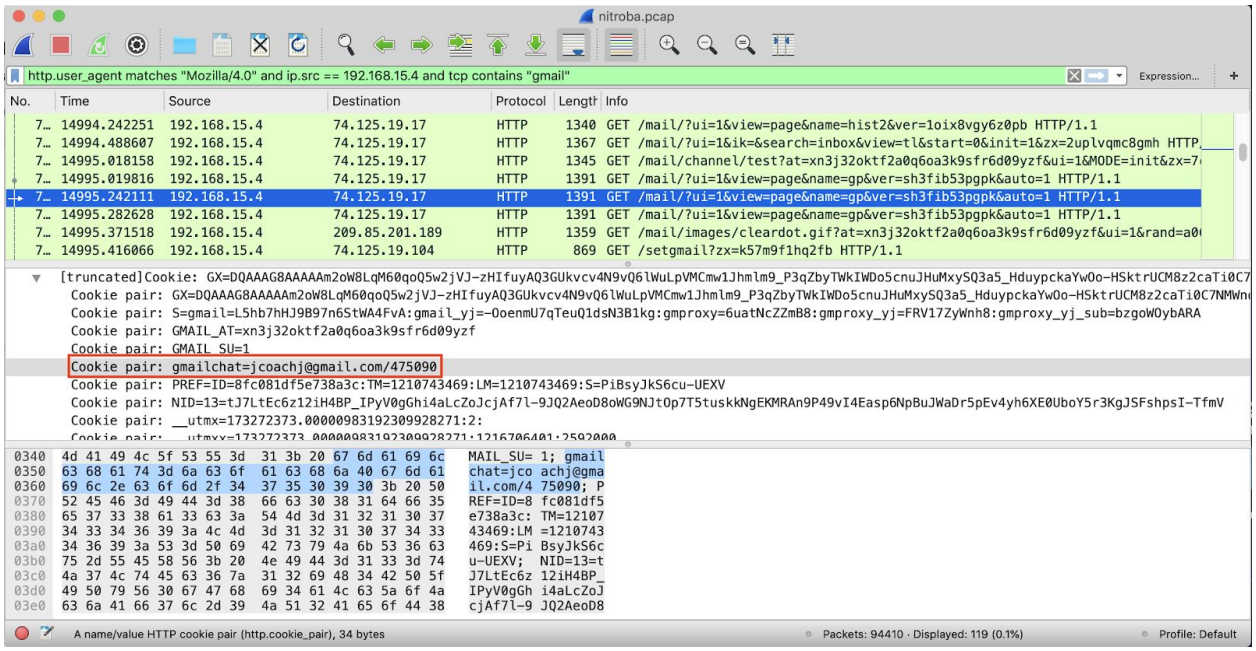
3) Next, looking at internet usage that contains the offending website “willselfdestruct”, we can see that it also originates from the same IP as the previous offending internet searches suggesting the user wants to harass a teacher and also has the same User-Agent.



4) Using the two filters “chat” and “gmail”, you can find multiple instances of gmail that has been accessed under the name “jcaoch@gmail.com” which is suggestive that Johnny Coach was the

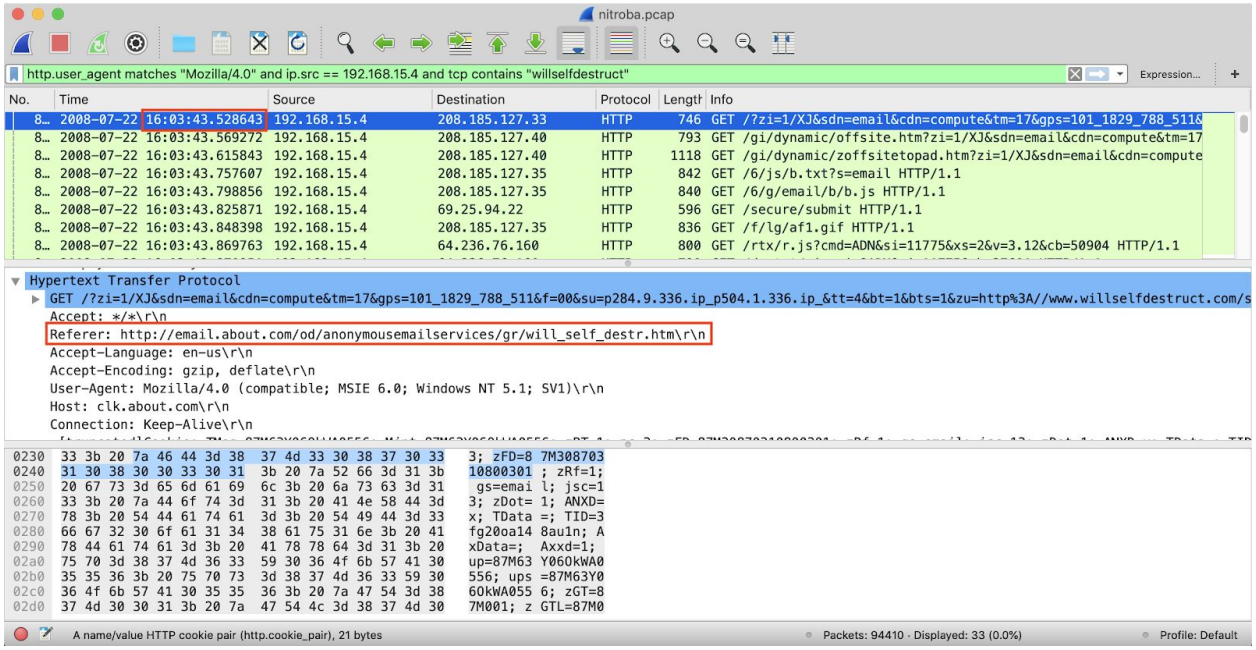
one who sent the harassment emails since he also logged in and used his email under the same IP.

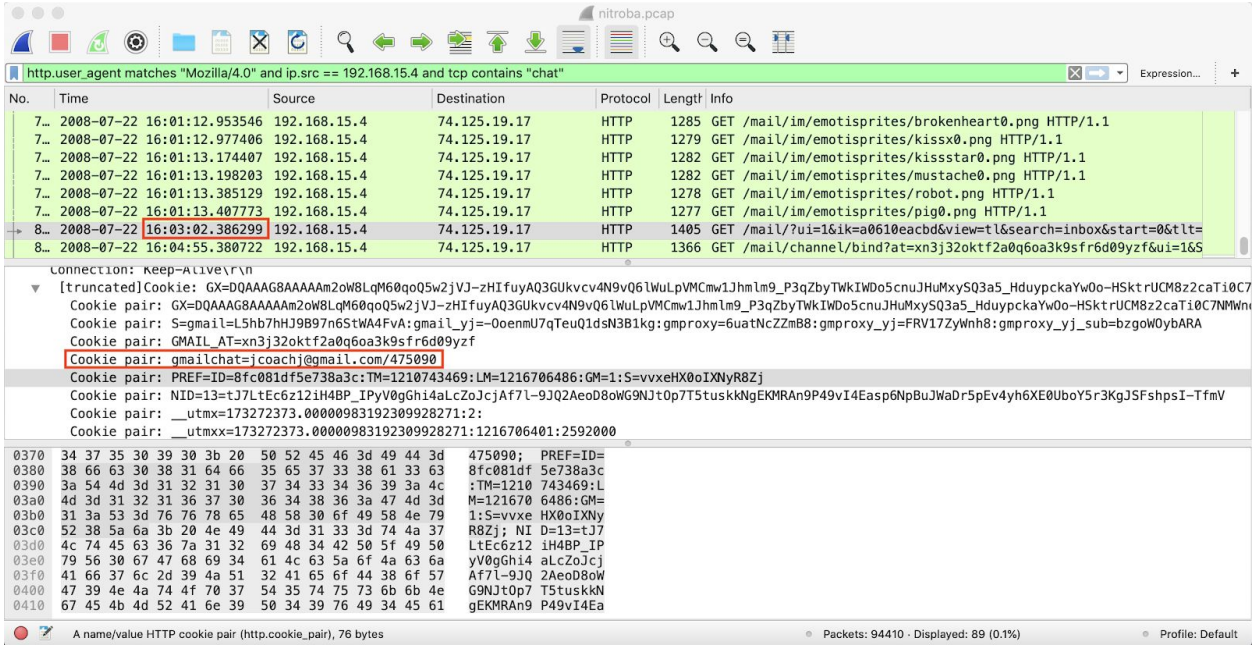


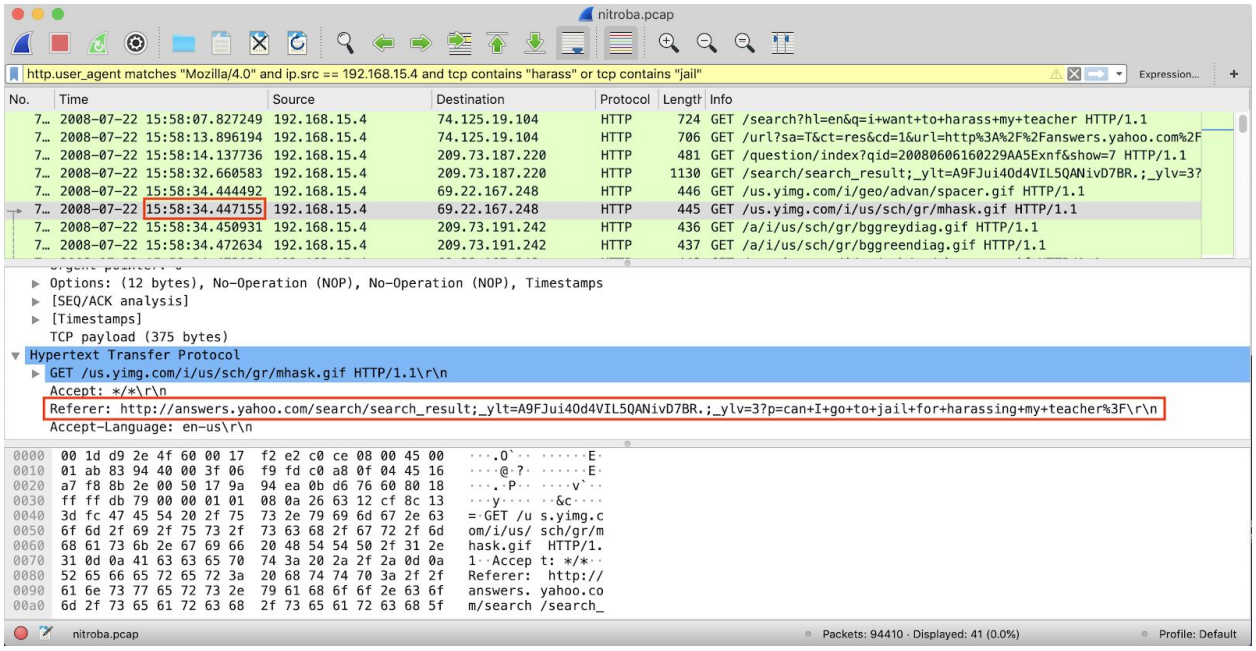


5) We then go to the “view” tab in wireshark, go to “time display format” and set it to show “Date and Time of Day” and repeat the searches done previously. In the “Time” column where it displays the time that each packet was sent, and hence when each search request to the internet was made, we can see that the time the willselfdestruct website was accessed is similar

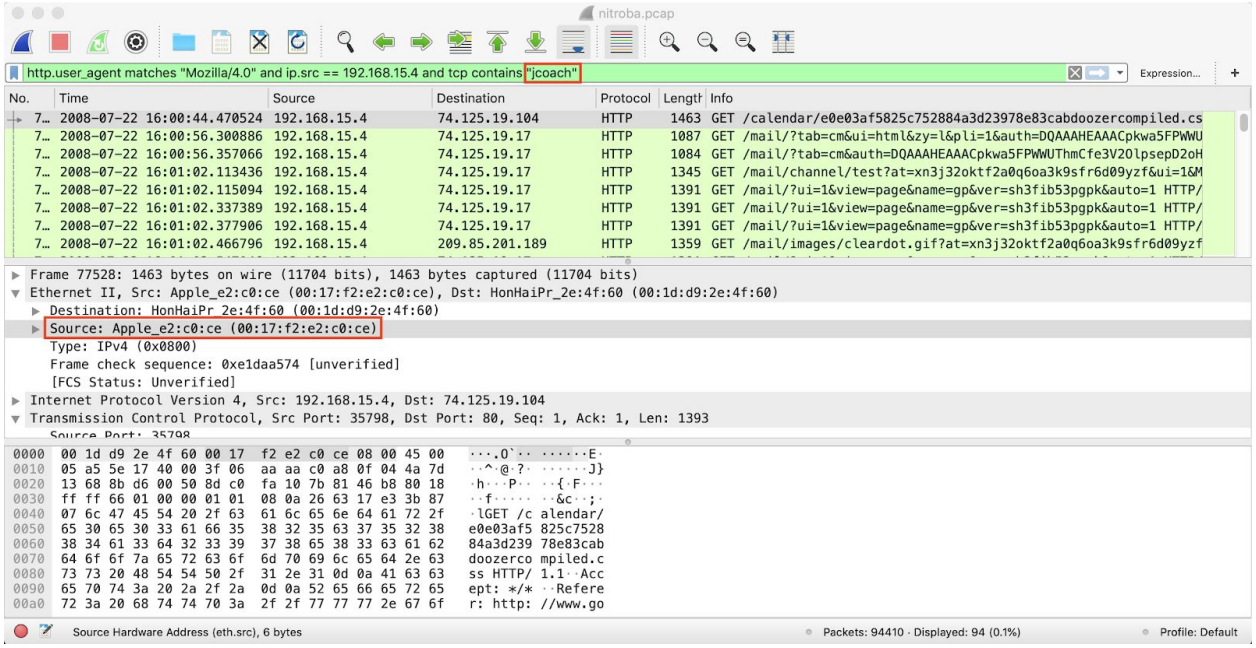
to when the email account "jcoach@gmail.com" was accessed and the incriminating searches such as "can I go to jail for harassing my teacher" was done.

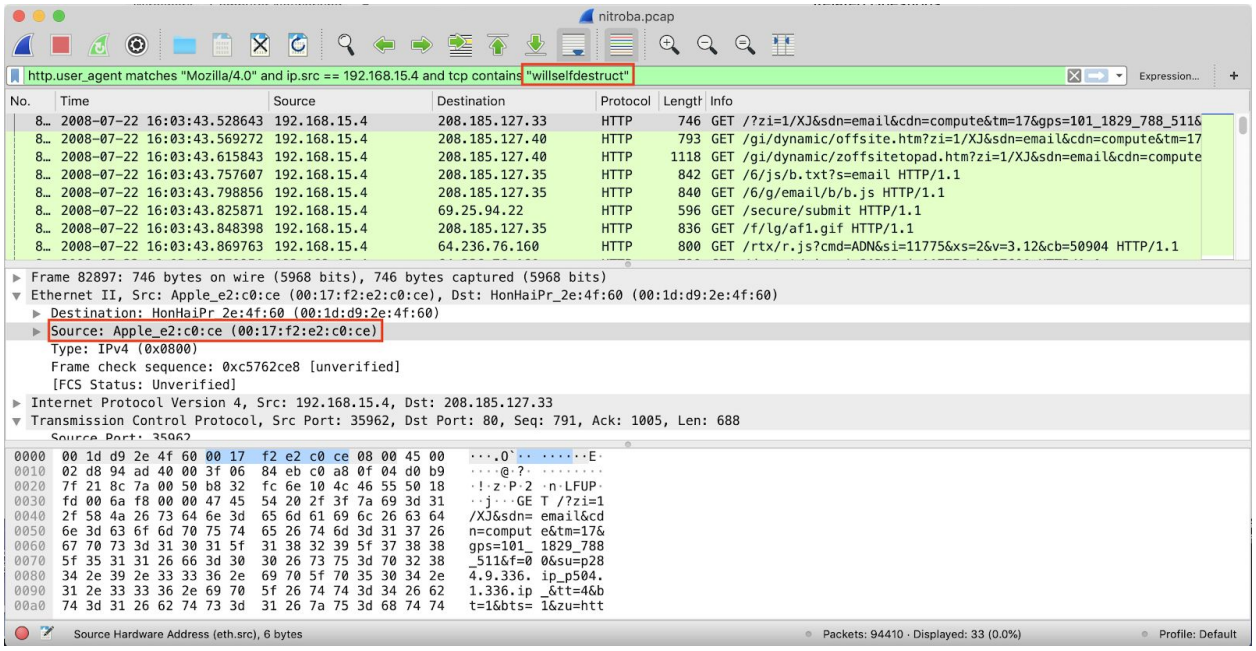






6) Lastly, if we access the Ethernet Source tab, which displays information about the device used, we can see that the MAC address, highlighted in a red box in the images below, are the same when accessing the email and the willselfdestruct website. MAC addresses are unique identifiers used to differentiate one device from another when on a network/ the internet. As such, we can link the usage of the site willselfdestruct to the use of Johnny Coach's email definitively, as IP addresses can be shared amongst many devices but MAC addresses are unique to each device.





7) Hence, on the balance of the probability that only Johnny Coach has access to his email address, and the fact that we can link the usage of the device to the usage of emails both based on device, software (web browser e.g internet explorer) and time, we can conclude that Johnny Coach was the one that sent the offending and harassing emails.

Limitations

1) Time - we were given approximately 6 weeks to complete this task on top of workload containing other things amongst this case study. As such, the investigation may not be as thorough.
2) Instructions - as this is a civil case and a search warrant was not obtained, we were unable to seize the suspect's devices to further prove that he was the one who sent the harassing emails to Tuckrige. Hence this report relies on the balance of probabilities, acceptable in civil cases, as opposed to "beyond reasonable doubt"

Declaration

1) I have read and understood the *Uniform Civil Procedure Rules 2005 - Schedule 7 - Expert Witness Code of Conduct* and agree to be bound by its terms.

2) My opinions expressed in this report is based wholly or substantially on my specialised knowledge referred to in this report.

3) I have made all enquiries that I believe are desirable and appropriate and no matters of significance which I regard as relevant have, to my knowledge, been withheld in this report.

Part 1B - Reflection Activity

1) What question(s) would you ask of your supervisor to ascertain that the PCAP file you have been asked to examine has been legally obtained (assume Nitroba is within NSW)?

In regards to this question, I will assume that legally obtained not only means that the evidence itself has been taken whilst compliant with the laws but also, it's admissibility in Court has been considered. Questions I would ask include:

- "Do you own or have you leased the network on which you have sniffed?" This is an important question as you can only legally sniff networks on which you owned/ have leased. Otherwise it would be considered "tapping" which is an illegal act.
- "Have you received or been granted permission by the owners of the network?" This would be asked if the previous question has been answered by a "no" since you would require permission to tap or tamper with other people's networks.
- "Is the network configured to be readily accessible to the general public? E.g unencrypted, etc." This question would be asked as it is legal to intercept connections that are publicly available.
- "Was the packet sniffing used for diagnostic purposes to ensure the efficient and effective maintenance of networks or to detect misuse?" This question should be asked as if the original intention of installing a network sniffer was to troubleshoot then it may be legal.
- "Have you received a search warrant clearance from the courts or some other form of higher authority or clearance such as a subpoena?" This question should be asked as the network sniffing may have been legally obtained if a valid warrant has been approved by the courts.

2) What would you do differently if this were a criminal case e.g Tuckrige complained to Police instead of the University,?

If this were a criminal case instead, there would have to be a formal procedure that should be followed. This involves the steps in prosecution including Investigation, Brief Assessment/ Decision to Charge, Charging or Commencing a Proceedings, Committal Proceeding, Hearing, Trial, Sentencing and Appeals. When dealing with a criminal case, one must appeal to the Courts or other parties of power for the authorisation of a search warrant and in that case, an investigator may forcibly seize any devices related to the crime at hand. However, as the current case is a civil case, no devices were taken into custody, and the Nitroba University themselves deemed network sniffing the ideal choice of tool in order to find incrimination evidence. Furthermore, more substantial, thorough and incrimination evidence may be formed in the case of a criminal case (e.g seizing of laptops and checking search histories, fingerprints, etc.) as the standard of proof on the prosecution must be "beyond reasonable doubt", however in a civil case such as the current, it lies on the balance of probability and hence the current evidence should suffice. Hence we are able to convict Coach on the basis of the balance of probability that since gmail requires a password and he was seen interacting on the IP address multiple times, that it was Coach that sent the harassing emails. This would not be an admissible conclusion in a criminal investigation. Lastly, in a criminal case the standard of information required it often higher and stricter procedures must be followed in order to maintain

admissibility although the evidence in both a criminal and civil case must ideally be deemed admissible, authentics, reliable, valid and credible. However, in contrast, in a civil case such as the Nitroba case, since the initial process of electronic discovery is enough to escalate the case to court (e.g screenshots of emails showing harassment) and hence the investigations in this report may be less formal than one that would require a criminal investigation.

References *(for Part 1B)*

Antwi-Boasiako, A. and Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. Advances in Digital Forensics XIII, pp.23–38.

Burgess Forensics. (2015). Computer Forensics - Criminal vs Civil: What's the Difference? - Burgess Forensics, accessed 26 October 2019, <https://burgessforensics.com/computer-forensics-criminal-vs-civil-whats-the-difference>

eSafety Commissioner. (2019). Legal assistance | eSafety Commissioner, accessed 27 October 2019, <https://www.esafety.gov.au/key-issues/image-based-abuse/legal-assistance>

KKIENERM (2019). Cybercrime Module 6 Key Issues: Digital Evidence Admissibility, accessed 27 October 2019, <https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html>

Part 2 - Extended Question

Section 146 of the Evidence Act states that “[evidence] that is produced completely or partly by a device or process that is tendered by a part who asserts that, in producing the document or thing, the device or process has produced a particular outcome”. Paragraph 2 of Section 146 also states that “if it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed … that, in producing the document or thing on the occasion in question, the device or process produced that outcome”. As such, many argue as Section 146 of the Evidence Act permits, believe that police may rely on tools such as Cellebrite UFED, XRY and Autopsy to assist in the collection of digital evidence, without the need for and as a replacement to digital expert testimonies as this would allow Police to cope with the operational pace of serious criminal investigations and the volume of work. However, the contrary is in fact true, and this is just a simple misinterpretation and manipulation of the views of the existing scenarios which has the negative impact of unreasonably shifting the burden of proof on the defendant. and as will be discussed later, the training required in order to ensure police are at a capable standard of interpreting auto-generated reports ultimately creates the same burden on taxpayers. Lastly, according to the australian crime prevention department states that mobile phone ownership has been increasing rapidly and between 2000 to 2010, the number of telephone services in operation has increased two-fold. As a result of mobile evidence being largely involved in crimes due to the recent influx of mobile usage, relying on section 146 unreasonably shifts the burden of proof to the defendant as the onus of proof is on the party seeking to establish the unreliability of evidence produced by a process, machine or device.

The first issue we will examine is the reliability and costs of replacing forensic experts with tools. In this case, we have chosen to examine Cellebrite’s Universal Forensic Extraction Device (UFED) which is the most widely acclaimed and recognised mobile forensic tool as of 2019, having won two Presidential awards in 2018 for the 10th year in a row. Cellebrite’s UFED is a tool compatible with over 2500 mobile devices and allows automated report generation as well as the ability to unlock any most modern devices and extract files, gain access to third party app data, chat conversations, downloads, deleted content and other forms of data from such mobile devices. Although this allows for automated mobile device cracking and report generation, the acquisition and maintenance of these devices are large. For example, in June 2019, Cellbrite made a contract with the U.S. Immigration and Customs Enforcement for approximately $30 to $35 million USD for “accessories licenses, training and support services” regarding the Cellebrite UFED tool for one year with the option to extend the contract up to 5 years for additional costs. For cost comparison, the official Parliament of Australia website states that in 2016-17 “$20.4 million AUD was invested over four years to increase the Australian Federal Police’s capability to combat cybercrime, as part of a broader package to implement the revised Cyber Security Strategy released in April 2016” and in 2018-19, “The Department of Parliamentary Services was allocated $9 million over four years to establish a Cyber Security Operations Centre for Parliament House”. Evidently, the large difference in money for using the UFED tool in comparison to the maintenance and construction of new measures for cyber

security must be obtained from a source and hence becomes a large burden on the taxpayer. Furthermore, although reports by NIST CFTT (National Institute of Standards and Framework's Cybersecurity Framework) conclude that “Cellebrite’s UFED performed consistently well during testing” and that “Connectivity issues between the UFED and phones tester were rare” it was stated that there were cases where “UFED only had difficulty connecting to certain GSM phones that did not contain a SIM card, and these issues most likely could be remedied by creating a cloned SIM card”. However, in this case, there is a level of digital expertise required in the solution proposed, expertise of which ordinary police would not have knowledge of and hence may cause negligence in evidence handling thus emphasising the need for digital forensic experts. Lastly, outsourcing to one external and centralised company such as Cellebrite as opposed to using internal digital forensic experts within the Australian Federal Police force or outsourcing to independent companies poses a major security risk in itself. It was reported that on 12th January 2017 900GB of confidential data was stolen from Cellebrite’s external servers including evidence files from seized mobile phones and logs from Cellebrite devices. To further this point, there was a scandal early 2019 UFED devices that have been used by federal agencies such as the police, FBI or Immagration and Customs Enforcement, were being sold on ebay for between $100 to $1000 USD without wiping them and instead of returning them to Cellebrite for proper decommissioning. This occurrence that could have been avoided if the current forensic outsourcing methods were used as opposed to trusting a big corporation’s new and unknown tooling and also concurrently emphasises the lack of digital knowledge by police and hence supports that digital forensic experts are crucial and their roles should not be substituted by police.

Advocaters for the idea of replacing the role of digital forensic experts with standard police suggest that it is the only way police can cope with the operational pace of serious criminal investigations and volume of work. However, this is conflicting and incorrect. This proposition places high liability on the police force, causing distractions from their important roles in gathering much of the physical evidence in often dangerous environments and hence a greater burden. An article by The Guardian states that “police are trampling over vital forensic evidence, are under-trained, and often do not know what they are looking for” a statement that puts emphasis on the inability for police to do the same work that digital forensic experts do due to lack of qualification and training. A specialist in discover forensics, Dr Jan Collie states in 2018 that “A lot of police stations have [mobile phone extraction kiosks] where they put a mobile phone in and press a couple of buttons, but it’s not enough analysis. A police officer who has been trained for about a day can use the equipment. He can click it in and handle the buttons, [but] often they spoil the evidence by mishandling. It’s like they have trodden on the evidence… they are not trained to do it” further stressing the amount of work that would have to be put in for police to be able to handle digital forensic evidence properly. In 2019, there was a London rape trial case that produced an unfair verdict, after police failed to recover photographs from a mobile phone after investigation for a year and a half that would have presented very clear evidence for the prosection. Similarly, another child sexual assault case in Decemeber was abandoned after evidence from the defendant’s phone was handed over late as the case was about to go to trial. As a result, a child rapist was cleared at court due to the lack of evidence.

These are just a few examples of cases where police were entrusted to handle digital evidence as opposed to requesting assistance from a forensic expert and as a result of malpractice and insufficient qualifications, court cases were mishandling, ultimately creating a burden on the police in the public eye for their mistakes. These mistakes could have been avoided if the police outsourced to digital forensic experts as opposed to handling work that they do not have expertise in themselves, as forensic experts could cope with the handling of digital evidence faster, more thoroughly and properly as it is what they have been trained in. Lastly, people may argue that with the introduction of new tools such as the Cellebrite UFED, this mishandling of evidence via the lack of evidence and slow turnover rate would not be an issue. However, there still lies the problem in the lack of expertise in police in their ability to properly interpret the evidence created by these auto-generating tools that may create reports containing evidence. For example, the 2010 case concerning George De La Cruz (De La Cruz) and Julie Ann Gonzalez (Gonzalez) in the Texas is a classic example of this where the police were led astray on a misleading trail due to their inability to process digital evidence. In this case, De La Cruz portrayed his wife as having ran away through posting misleading messages on social media indicating she had done so on her phone after he had murdered her due to anger at a potential divorce. It was not until 3 years later, with the aid of digital forensic experts that they found out that De La Cruz had been the man behind the crime, hence accentuating the need for the digital forensic expert role.

Finally, replacing experts with police is a harmful idea as it introduces a large bias which ultimately places a large responsibility to procure proof on the defendant as opposed to the prosecutor. The failure to produce accurate and reliable evidence by the prosecutor threatens the fairness of a court case trial. Furthermore, the inability for police to understand terminology in the field of digital expertise may also hinder the jury's perspective and understanding of the trial at hand. For example, a simple concept such as hashing images may not be understood by police and although may be done automatically by the automated tooling, the lack of understanding by the police may as a result lead to police being unable to confidently and properly explain the process of evidence acquisition to the jury and hence lead to scepticism or event inadmissibility of evidence. Furthermore, police spending on forensics in England has halved in the last 10 years leading to many news headlines emphasising the negative consequences including "Police forensic science at 'breaking point', warn peers", "Justice system at 'breaking point' over digital evidence", "Forensic Science in Crisis" or even "Police mishandling digital evidence, forensic experts warn". This is a great example of the detriments to the legal system that removing and replacing digital forensic experts with police would cause, ultimately burdening society and the credibility of its legal system.

Overall, police can not replace digital forensic experts and the many benefits outlined by supporters of this idea are misinformed in their ideas. Replacing experts with police does not ease the pace of investigations as requiring police to learn how to interpret reports from automated tooling can cause lengthy delays in prosecuting serious crimes themselves and can cause legal issues as police are not reasonable necessarily interpreters of these reports, and shifts the burden of proof unfairly towards the defendant and is ultimately creates a burden on

the taxpayer. Arguing that police and digital forensic experts are both under the category of law enforcement and hence labelling them as interchangeable is an unreasonable assumption and would be the equivalent of replacing lawyers, who are also law enforcers, with police under the argument of relieving the volume of work from police, an absurd idea. Digital forensic experts play an important role in ensuring a fair trial and aid police in their investigations, by releasing them of the burden of having to deal with the realm of digital evidence, allowing them to focus on the criminal investigations at hand and hence also alleviating the obligations of taxpayers and liability on the police.

References *(for Part 2)*

APH (2016). Law enforcement and crime prevention – Parliament of Australia, accessed 20 October 2019, <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201617/LawEnforce>

APH (2018). Cyber policy – Parliament of Australia, accessed 23 October 2019, <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201819/CyberPolicy>

Augenstein, S. (2018). The Digital Forensic Boom, Forensic Magazine, accessed 2 November 2019, <https://www.forensicmag.com/article/2018/06/digital-forensic-boom>

Author Unknown. Preparing Testimony about Cellebrite UFED in a Daubert or Frye Hearing. (n.d.), Accessed 1 November 2019, <http://www.kmbllaw.com/wp-content/uploads/CellebritePreparingtoTestifyArticle.pdf>

Author Unknown (2014). John Irvine Offers Tips and Insights on a Digital Forensics Career, The Balance Careers, accessed 2 November 2019, <https://www.thebalancecareers.com/what-it-s-like-to-work-as-a-digital-forensic-examiner-974889>

Author Unknown. (2019). Digital Forensics Poses Challenges for Texas Law Enforcement, accessed 2 November 2019, <https://www.govtech.com/public-safety/Digital-Forensics-Poses-Challenges-for-Texas-Law-Enforcement.html>

Author Unknown. (2019). Fighting Cybercrime: Cybersecurity and Digital Forensics Are the New A-Team | Sponsored Content | TechNewsWorld, accessed 2 November 2019, <https://www.technewsworld.com/story/86198.html>

Bowcott, O. (2018). Police mishandling digital evidence, forensic experts warn, the Guardian, accessed 2 November 2019,

<https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn>

Bowcott, O. (2018). Justice system at “breaking point” over digital evidence. [online] the Guardian, accessed 2 November 2019 , <https://www.theguardian.com/law/2018/feb/12/justice-system-at-breaking-point-over-digital-evidence>

Cellebrite. (2017). Cellebrite, accessed 20 October 2019 <https://www.cellebrite.com/en/ufed-ultimate>

Clive Cookson (2019). Police forensic science at ‘breaking point’, warn peers, accessed 2 November 2019, <https://www.ft.com/content/f3336774-6b4c-11e9-a9a5-351eeaef6d84>

Devlin, H. (2018). Police outsource digital forensic work to unaccredited labs, accessed 2 November 2019, <https://www.theguardian.com/uk-news/2018/feb/12/police-outsource-digital-forensic-work-to-unaccredited-labs>

Mohamad, H. (2011). Background paper: mobile phone crime, accessed 19 October 2019, <http://www.crimeprevention.nsw.gov.au/Documents/mobile_phone_crime_background_paper.pdf>

PrivSec Report. (2019). New tool by Cellebrite can unlock any iPhone - PrivSec Report, accessed 1 November 2019, <https://gdpr.report/news/2019/06/18/new-tool-ellebrite>

ThemeGrill (2012). Computer Forensics | Australian Police, accessed 2 November 2019, <https://www.australianpolice.com.au/forensic-scientists/computer-forensics>

Wilson, T.J. (2019). Forensic science is in crisis – and this could have critical effects on UK legal system, accessed 2 November 2019, <http://theconversation.com/forensic-science-is-in-crisis-and-this-could-have-critical-effects-on-uk-legal-system-113873>

Yaron Steinbuch (2019). You can buy the feds’ favorite phone hacking tool for $100 on eBay, accessed 29 October 2019, <https://nypost.com/2019/02/27/you-can-buy-the-feds-favorite-phone-hacking-tool-for-100-on-ebay>