



Sniffer

- محتوى الكتاب

- مقدمة عن السنايفر

- طريقة عمل سنايفر من خلال برنامج Wire Shark

بسم الله الرحمن الرحيم :

السنايفر هي عملية تستخدم برنامج ما للقيام بعملية تجسس على اتصالات موجودة في الشبكة او ما يسمى التقاط كامل لاي داتا تمر من خلال كارت الشبكة , السنايفر يقوم بتحويل كرت الشبكة المركبة على الجهاز الى وضعية الأستقبال ليتم الألتقاط اي داتا تمر من خلال الشبكة

فبعد تحويل كرت الشبكة لوضعية الألتقاط يقوم البرنامج بتحليل هذه البيانات ويطرحها لنا على شكل اكواد مشفرة , يتم فك تشفيرها بعد ذلك للحصول على البيانات بشكل سليم السايفر يكون على بروتوكولات اتصال مختلفة مثل :

- HTTP
- POP
- FTP
- SMTP

WireShArK

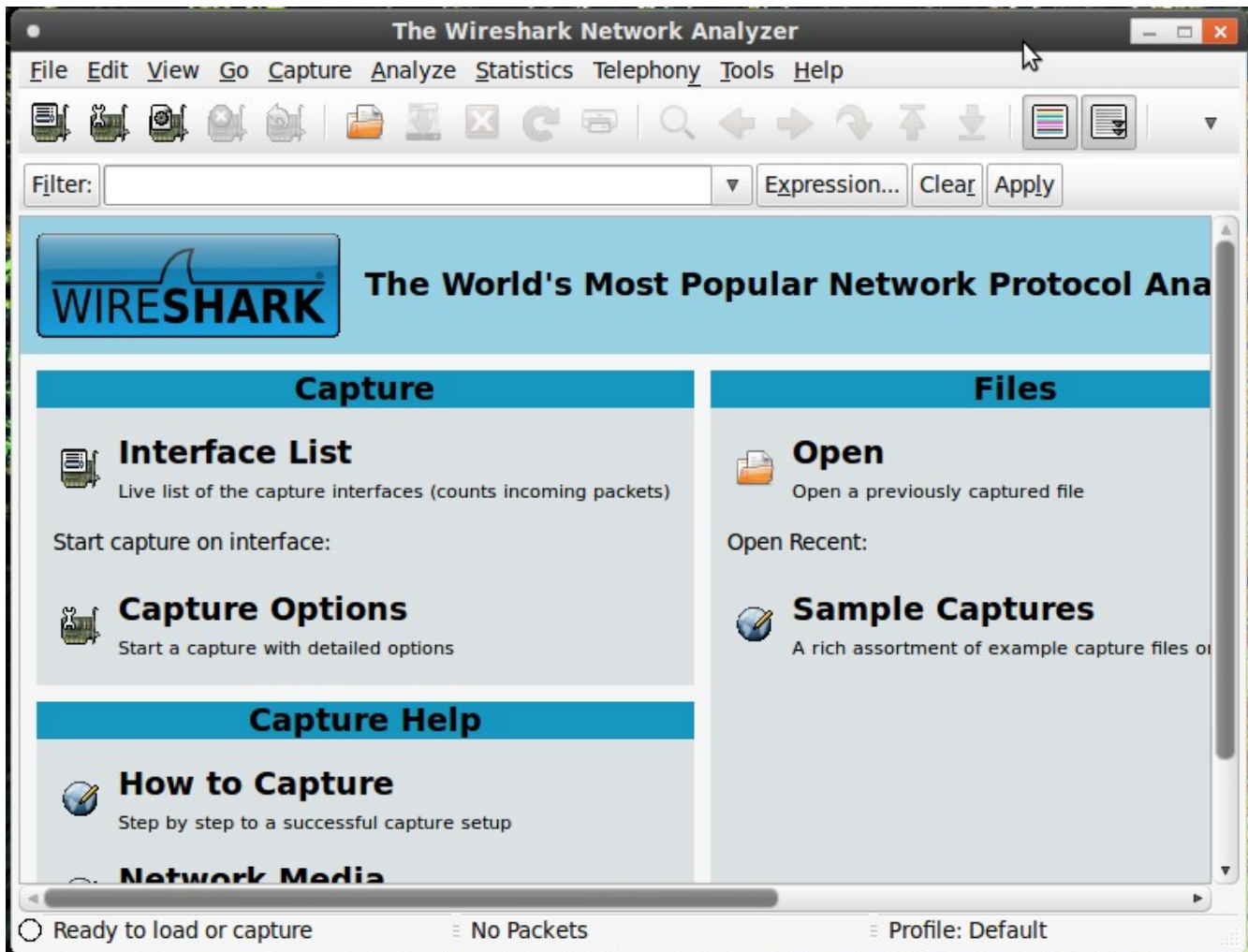


يعتبر هذا البرنامج من افضل البرامج التي تستخدم للأتقاط كلمات المرور في السنيف

تنصيب البرنامج على ابونتو:

```
sudo apt-get install wireshark
```

واجهة البرنامج



شرح طريقة الاستخدام

نقوم في البداية بالدخول الى الطرفية بصلاحيه الجذر

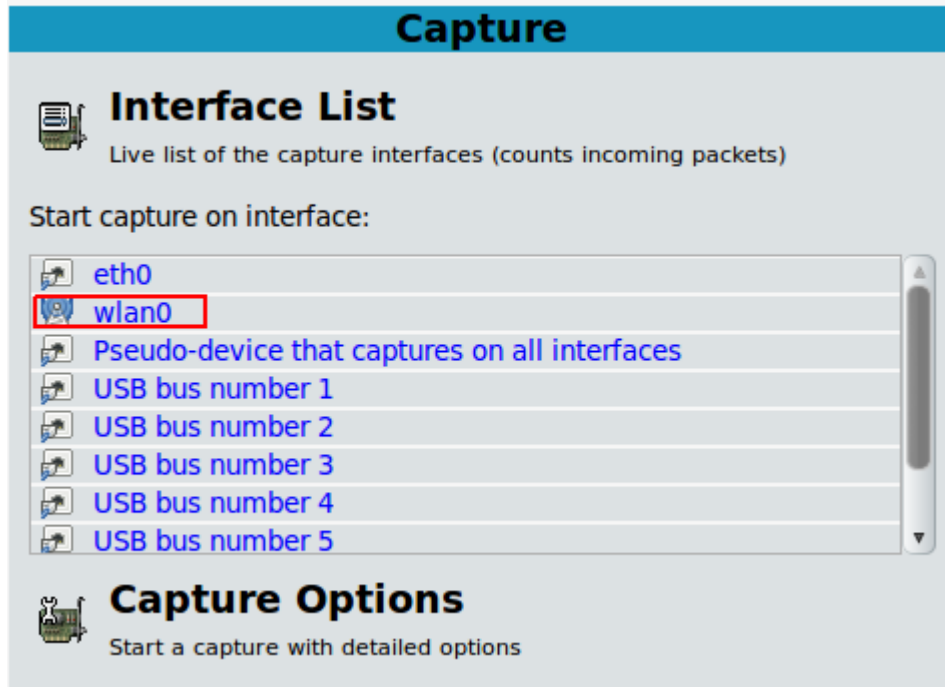
```
sudo -i
```

وبعد ذلك نقوم بتشغيل البرنامج بالامر التالي

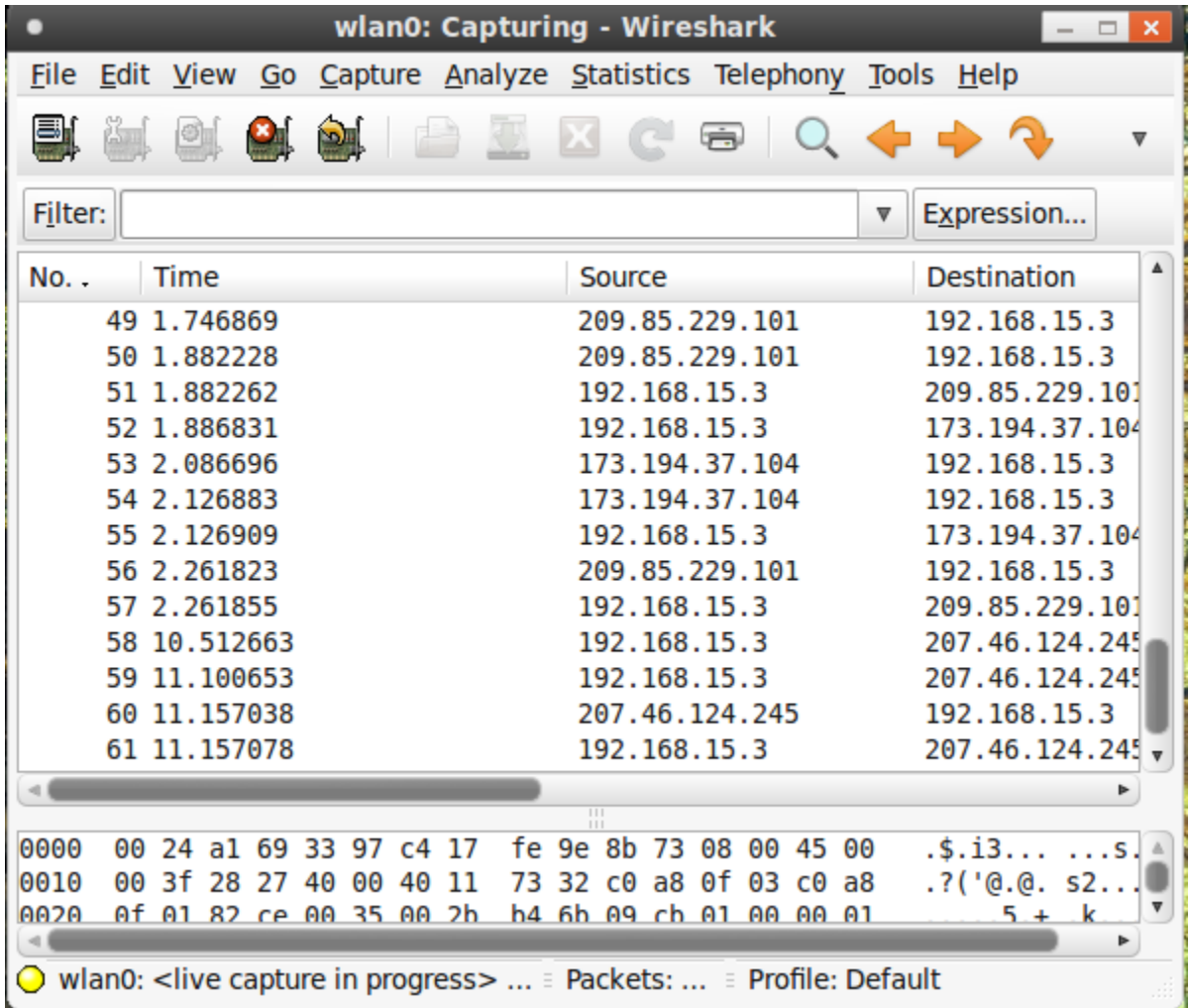
```
ubuntu@rOck-laptop:~$ cd ..
```

```
ubuntu@rOck-laptop:/home$ wireshark
```

بعد تشغيل البرنامج نقوم باختيار الاتصال المستخدم لديك في الجهاز وبما انني استخدم اتصال الوايرلس فسيكون الاختيار على الشكل التالي

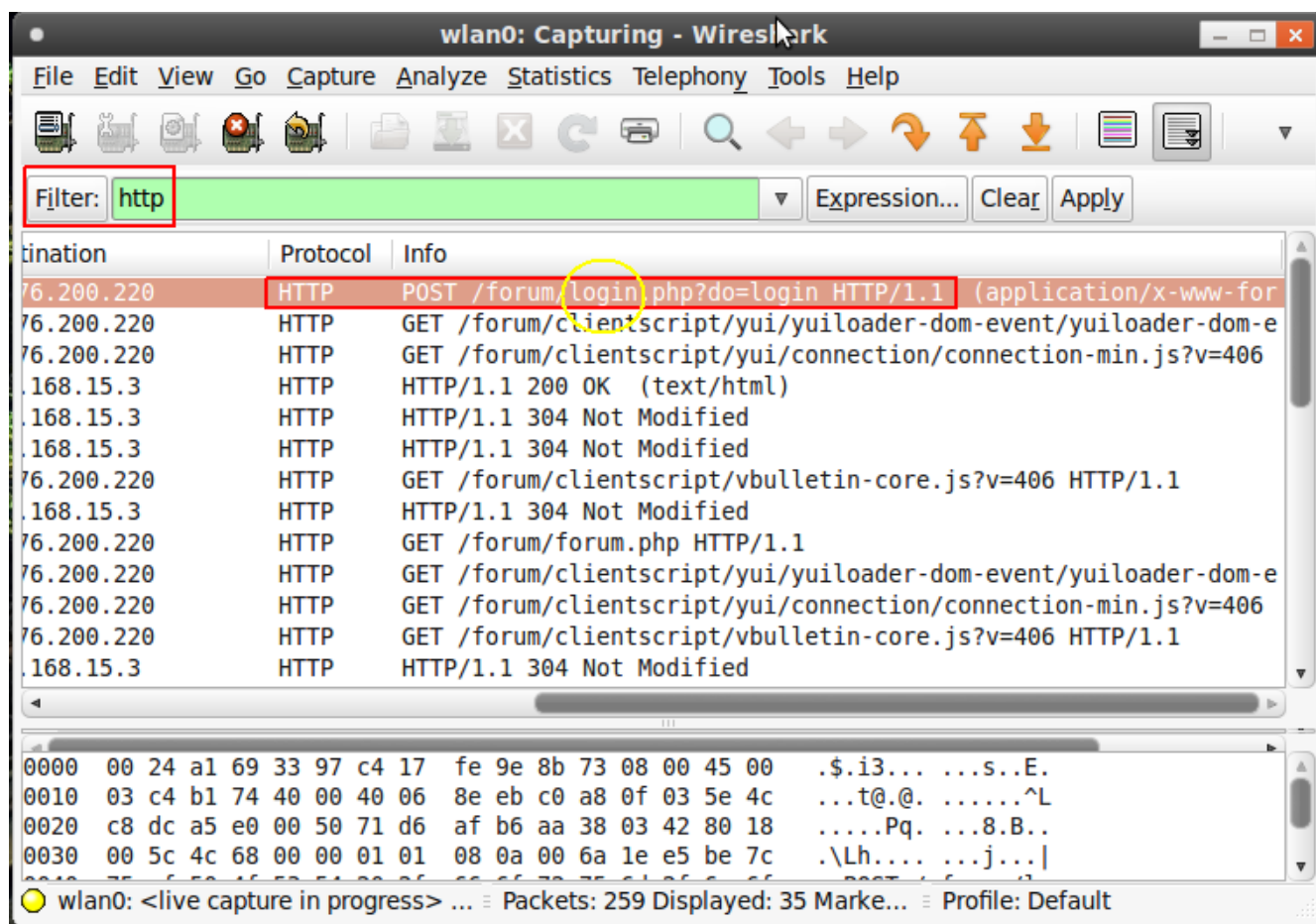


بعد ذلك ستفتح واجهة البرنامج التي تظهر بها جميع عمليات الاتصال والتي يتم من خلالها
التقاط البيانات



مثال عملي

قم بالدخول لاي موقع مسجل انت فيه كمنتدى او بريد الكتروني . قمت انا بالتجربة على عضويتي في مجتمع لينوكس العربي . نتابع بعد قيامنا بالدخول نتوجه للبرنامج وبما ان كلمة المرور المراد سحبها متعلقة في بروتوكول من نوع HTTP



The screenshot shows the Wireshark interface with a filter set to 'http'. The packet list pane displays several HTTP requests and responses. The first packet is highlighted in red and circled in yellow, showing a POST request to '/forum/login.php?do=login'. The packet bytes pane shows the raw data of the captured packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	76.200.220	76.200.220	HTTP	1000	POST /forum/login.php?do=login HTTP/1.1 (application/x-www-form-urlencoded)
2	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/clientscript/yui/yuiloader-dom-event/yuiloader-dom-event.js?v=406 HTTP/1.1
3	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/clientscript/yui/connection/connection-min.js?v=406 HTTP/1.1
4	0.000000	168.15.3	168.15.3	HTTP	1000	HTTP/1.1 200 OK (text/html)
5	0.000000	168.15.3	168.15.3	HTTP	1000	HTTP/1.1 304 Not Modified
6	0.000000	168.15.3	168.15.3	HTTP	1000	HTTP/1.1 304 Not Modified
7	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/clientscript/vbulletin-core.js?v=406 HTTP/1.1
8	0.000000	168.15.3	168.15.3	HTTP	1000	HTTP/1.1 304 Not Modified
9	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/forum.php HTTP/1.1
10	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/clientscript/yui/yuiloader-dom-event/yuiloader-dom-event.js?v=406 HTTP/1.1
11	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/clientscript/yui/connection/connection-min.js?v=406 HTTP/1.1
12	0.000000	76.200.220	76.200.220	HTTP	1000	GET /forum/clientscript/vbulletin-core.js?v=406 HTTP/1.1
13	0.000000	168.15.3	168.15.3	HTTP	1000	HTTP/1.1 304 Not Modified

Packet bytes pane (hex and ASCII):

```
0000  00 24 a1 69 33 97 c4 17 fe 9e 8b 73 08 00 45 00  .$.i3... ..s..E.
0010  03 c4 b1 74 40 00 40 06 8e eb c0 a8 0f 03 5e 4c  ...t@.@. ....^L
0020  c8 dc a5 e0 00 50 71 d6 af b6 aa 38 03 42 80 18  ....Pq. ...8.B..
0030  00 5c 4c 68 00 00 01 01 08 0a 00 6a 1e e5 be 7c  .\Lh.... ...j...|
```

8 23.944689 192.168.15.3 94.76.200.220 HTTP POST /fo

- + Frame 8 (978 bytes on wire, 978 bytes captured)
- + Ethernet II, Src: HonHaiPr_9e:8b:73 (c4:17:fe:9e:8b:73), Dst:
- + Internet Protocol, Src: 192.168.15.3 (192.168.15.3), Dst: 94.7
- + Transmission Control Protocol, Src Port: 42464 (42464), Dst Po
- + Hypertext Transfer Protocol
- Line-based text data: application/x-www-form-urlencoded
[truncated] vb_login_username=r0ckHunter&vb_login_password=

USER

```
0000  00 24 a1 69 33 97 c4 17 fe 9e 8b 73 08 00 45 00  .$.i3
0010  03 c4 b1 74 40 00 40 06 8e eb c0 a8 0f 03 5e 4c  ...t@
0020  c8 dc a5 e0 00 50 71 d6 af b6 aa 38 03 42 80 18  ....!
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

8 23.944689 192.168.15.3 94.76.200.220 HTTP POST /fo

_login_md5password=827ccb0eea8a706c4c34a16891f84e7b&vb_login_md5

Pass Word

```
a1 69 33 97 c4 17 fe 9e 8b 73 08 00 45 00  .$.i3... ...s..E.
b1 74 40 00 40 06 8e eb c0 a8 0f 03 5e 4c  ...t@.@. ....^L
a5 e0 00 50 71 d6 af b6 aa 38 03 42 80 18  ....Pq. ...8.B..
```

بعد استخراج الـيوزر وكلمة المرور مشفرة من نوع (Md5)
قم بفك التشفير من خلال اي موقع لفك التشفير او استخدام برنامج لفك التشفير كالجوهن

rOckHuntEr
r0ck.hunt3r@gmail.com

جميع الحقوق محفوظة للكاتب يتم نشر الكتاب مع ذكر المصدر