NetworkMiner ile Trafik Analizi

Wireshark'ı açtığımızı, bir interface seçtiğimizi ve Start butonuna basarak sniffing'e başladığımızı varsayalım.



Paketler ekrana akmaya başlayacaktır.

| | Capturing from ethO [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)] | | | | | | |
|---|---|---|--------------------------|------------------------------|---------------|--|--|
| File | Ec | lit View Go | Capture Analyze Stat | stics Telephony Tools | Internals Hel | P | |
| 0 | ۲ |) 🛋 🔳 🙋 | (🖴 🛅 💥 🤁 | Q + + 7 T : | | e o d 🖭 🕁 💟 🍢 🖬 🔀 | |
| Filte | er: | | | ~ Expressio | on Clear App | oly Save | |
| No. | | Time | Source | Destination | Protocol Len | igti Info | |
| | 1 | 0.000000000 | CadmusCo_90:ba:f8 | Arcadyan_54:3d:bd | ARP | 42 192.168.2.2 is at 08:00:27:90:ba:f8 | |
| | 2 | 0.019782000 | CadmusCo_90:ba:f8 | AsustekC_64:a9:d5 | ARP | 42 192.168.2.1 is at 08:00:27:90:ba:f8 (duplica | |
| | Э | 2.000395000 | CadmusCo_90:ba:f8 | Arcadyan_54:3d:bd | ARP | 42 192.168.2.2 is at 08:00:27:90:ba:f8 | |
| | 4 | 2.020247000 | CadmusCo_90:ba:f8 | AsustekC_64:a9:d5 | ARP | 42 192.168.2.1 is at 08:00:27:90:ba:f8 (duplica | |
| | 5 | 3.716051000 | 192.168.2.2 | 173.194.44.1 | TCP | 66 46452 > https [ACK] Seq=1 Ack=1 Win=474 Len=(| |
| | 6 | 3.716132000 | 192.168.2.5 | 192.168.2.2 | ICMP | 94 Redirect (Redirect for host) | |
| | | | | | | 66 [TCP Dup ACK 5#1] 46452 > https [ACK] Seq=1 , | |
| | | | | | | 66 [TCP ACKed unseen segment] https > 46452 [AC | |
| | | 3.805418000 | 173.194.44.1 | | TCP | 66 [TCP Dup ACK 8#1] [TCP ACKed unseen segment] | |
| | 10 | 4.000908000 | CadmusCo_90:ba:f8 | Arcadyan_54:3d:bd | ARP | 42 192.168.2.2 is at 08:00:27:90:ba:f8 | |
| | 11 | 4.020812000 | CadmusCo_90:ba:f8 | AsustekC_64:a9:d5 | ARP | 42 192.168.2.1 is at 08:00:27:90:ba:f8 (duplica | |
| | 12 | 4.154321000 | 192.168.2.1 | 239.255.255.250 | SSDP | 368 NOTIFY * HTTP/1.1 | |
| | 13 | 4.154610000 | 192.168.2.1 | 239.255.255.250 | SSDP | 370 NOTIFY * HTTP/1.1 | |
| | 14 | 4.154621000 | 192.168.2.1 | 239.255.255.250 | SSDP | 380 NOTIFY * HTTP/1.1 | |
| | 15 | 4.154941000 | 192.168.2.1 | 239.255.255.250 | SSDP | 374 NOTIFY * HTTP/1.1 | |
| • Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0 • Ethernet II, Src: CadmusCo_90:ba:f8 (08:00:27:90:ba:f8), Dst: Arcadyan_54:3d:bd (00:12:bf:54:3d:bd) • Address Resolution Protocol (reply) • • • • • • • • • • • • • • • | | | | | | | |
| 0 💅 | eth | n0: <live capture<="" td=""><td>e in progress> Fil Packe</td><td>ts: 96 · Displayed: 96 (100.</td><td>0%)</td><td>Profile: Default</td></live> | e in progress> Fil Packe | ts: 96 · Displayed: 96 (100. | 0%) | Profile: Default | |

Diyelim ki includekarabuk'ün admin paneline giriyoruz.

www.includekarabuk.com/adminPaneli/index.php

Kullanıcı adı ve şifreyi girdikten sonra Wireshark'a dönelim. Girdiğimiz kullanıcı adı ve şifreyi taşıyan paketi bulmak için yapabileceğimiz en iyi şey Wireshark filtrelerini kullanmak olucaktır. Dolayısıyla includekarabuk'ün IP'si üzerinden bir paket filtreleme yapalım. Bunun için önce includekarabuk'ün IP'sini öğrenelim.

> nslookup www.includekarabuk.com

Output:

93.89.224.247

Ardından Wireshark filtresini hazırlayalım ve Wireshark'taki ilgili kutucuğua girelim:

ip.src == 93.89.224.247

| | Capturing from eth0 | [Wireshark 1.10.2 (S) | N Rev 51934 | from /trunk-1.10)] |
|-------------------------|----------------------|------------------------|--------------|--------------------|
| File Edit View Go | Capture Apalyze Stat | istics Telephony Tools | Internals H | elp |
| | | | | |
| | | | | |
| Filter: ip.src == 93.89 | 9.224.247 | ~ Express | sion Clear A | pply Save |
| No. Time | Source | Destination | Protocol Le | ngtl Info |
| 1640 342.9817850 | (93.89.224.247 | 192.168.2.2 | HTTP | 1112 [TCP Retransm |
| 1647 343.1093810 | (93.89.224.247 | 192.168.2.2 | TCP | 60 http > 45847 |
| 1648 343.1094060 | (93.89.224.247 | 192.168.2.2 | TCP | 54 [TCP Dup ACK |
| 1649 343.1251280 | (93.89.224.247 | 192.168.2.2 | TCP | 60 http > 45846 |
| 1650 343.1251510 | (93.89.224.247 | 192.168.2.2 | TCP | 54 [TCP Dup ACK |
| 1653 344.5773140 | (93.89.224.247 | 192.168.2.2 | HTTP | 280 HTTP/1.1 304 |
| 1654 344.5773660 | (93.89.224.247 | 192.168.2.2 | HTTP | 280 [TCP Retransm |
| 1658 344.7588690 | (93.89.224.247 | 192.168.2.2 | HTTP | 279 HTTP/1.1 304 |
| 1659 344.7589190 | (93.89.224.247 | 192.168.2.2 | HTTP | 279 [TCP Retransm |
| 1784 358.4447890 | (93.89.224.247 | 192.168.2.2 | TCP | 60 http > 45848 |
| 1785 358.4449100 | (93.89.224.247 | 192.168.2.2 | TCP | 54 [TCP Out-Of-O |
| 1907 389.6882860 | (93.89.224.247 | 192.168.2.2 | TCP | 60 [TCP Window U |
| 1908 389.6883160 | (93.89.224.247 | 192.168.2.2 | TCP | 54 [TCP Keep-Ali |
| 1911 389.8755580 | (93.89.224.247 | 192.168.2.2 | TCP | 60 [TCP Window U |
| 1912 389.8756120 | (93.89.224.247 | 192.168.2.2 | TCP | 54 [TCP Keep-Ali |

Enter'ladığımız takdirde sadece includekarabuk'e ait paketleri görür hale geliriz. Şimdi göz kararınca includekarabuk'e ait paketler arasından HTTP POST paketi arayalım.

| Wires | ark | | | | ti Tr 🖇 📧 🗤) 08:57 🔱 |
|----------|--|------------------------|---|-------------------------------|----------------------|
| 0 | 😣 🖻 💿 Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 f | rom master-1.10)] | | | |
| | File Edit View Go Capture Analyze Statistics Telephony | ools Internals Help | | | |
| | 🖲 🐵 🚄 🔳 🙇 🚞 🗎 🗶 C 🔍 🔇 | > 3 7 7 | | 🏭 🕅 🐚 💥 🔞 | |
| 9 | Filter: ip.src == 93.89.224.247 | Expression Clear | Apply Save | | |
| | No. Time Source Destination | on Protocol | Lengtł Info | | |
| K | 815 11.667556000 192.168.0.12 93.89.224 | .247 TCP | 54 49853 > http [ACK] Seq=1 Ad | ck=1 Win=29200 Len=0 | |
| 9 | 810 11.007/88000 192.108.0.12 93.89.224 831 11.737640000 93.89.224.247 192.168.0 | .12 TCP | 481 GET / adminPanell/index.pnp 60 http > 49853 [ACK] Seg=1 Ad | ck=428 Win=27740 Len=0 | |
| | 833 11.771267000 93.89.224.247 192.168.0 | .12 HTTP | 1176 HTTP/1.1 200 OK (text/htm | l) | |
| | 834 11.771296000 192.168.0.12 93.89.224 | .247 TCP | 54 49853 > http [ACK] Seq=428 | Ack=1123 Win=31416 Len=0 | |
| | 840 11.877396000 192.168.0.12 93.89.224 | .247 HTTP | 484 GET /favicon.ico HTTP/1.1 | | |
| | 846 11 943249889 93 89 224 247 192 168 8 | 12 ICP 12 HTTP | 1028 HTTP/1 1 404 Not Found (1) | ext (html) Mark Packet (tog | gle) |
| | 847 11.943277000 192.168.0.12 93.89.224 | .247 TCP | 54 49853 > http [ACK] Seq=858 | Ack=2097 Ignore Packet (to | ggle) |
| | 1155 17.673075000 192.168.0.12 93.89.224 | .247 HTTP | 770 POST /adminPaneli/index.php | p HTTP/1.1 Set Time Reference | e (toggle) 1) |
| | 1156 17.737178000 93.89.224.247 192.168.0 | .12 TCP | 60 http > 49853 [ACK] Seq=209 | 7 Ack=1574 Time Shift | |
| | 115/ 1/.856/55000 93.89.224.24/ 192.168.0 1158 17 856788000 192 168 0 12 93 89 224 | 247 TCP | 13/3 HTTP/1.1 200 OK (Text/ntm 54 49853 > http [ACK] Seg=1574 | Ack=3416 Packet Comment. | |
| 2 | 1236 62.866555000 192.168.0.12 93.89.224 | .247 TCP | 54 [TCP Keep-Alive] 49853 > h | ttp [ACK] Manually Resolve | Address |
| 60 | | | interfere 0 | Apply as Filter | |
| | ▶Frame 1155: 7/0 bytes on wire (6160 bits), 7/0 bytes ▶Ethernet II. Src: Asustek(64:a9:d5 (20:cf:30:64:a9: | d5) Dst: Broadcom de: | ad:05 (00:10:18:de:ad:05) | Prepare a Filter | |
| Z | ▶ Internet Protocol Version 4, Src: 192.168.0.12 (192. | 168.0.12), Dst: 93.89. | 224.247 (93.89.224.247) | Conversation Filte | er 🕨 |
| | Transmission Control Protocol, Src Port: 49853 (4985) | 3), Dst Port: http (80 |), Seq: 858, Ack: 2097, Len: 716 | Colorize Conversa | ition ► |
| | Hypertext Transfer Protocol | 1-1 | 사망 전 119 2 4 12 12 14 14 14 14 14 14 14 14 14 14 14 14 14 | SCTP | • |
| wel. | ▶Line-based text data: application/x-www-form-urlencd | led | | Follow TCP Stream | n |
| | | | | Follow UDP Strea | n |
| 2 | | | | Follow SSL Stream | ı |
| | 0000 00 10 18 de ad 05 20 cf 30 64 a9 d5 08 00 45 0 | 0dE. | | Сору | • |
| | 0010 02 f4 30 7a 40 00 40 06 08 85 c0 a8 00 0c 5d 5 |)0z@.@]Y | | Protocol Preferer | ices 🕨 🚽 |
| 1 | 0020 e0 f7 c2 bd 00 50 0c fe 7f 3a 3d 44 59 e1 50 1 | P:=DY.P. | | Decode As | |
| - | 0030 03 7C 01 CC 00 00 30 41 33 34 20 21 01 04 00 0 | nPaneli/ index nh | | Print | |
| | 🕽 💆 Ready to load or capture 🛛 🛛 Packets: 4539 · Di | played: Profile: De | fault | Show Packet in Ne | ew Window |

Görüldüğü üzere bir tane HTTP POST paketi bulduk. Şimdi ona sağ tıklayalım ve Follow TCP Stream diyelim. Böylece tıkladığımız paketin içini okuyabilelim.



Ve işte sonuç: userID=hefese&userPassword=tuzlucayir. Görüldüğü gibi kullanıcı adı ve şifre bilgisine biraz paketler üzerinde göz gezdirme yaparak ulaşabildik. Peki milyonlarca paket olsaydı...?

NetworkMiner Wireshark, tcpdump gibi trafik sniff'leyen araçlardan gelen trafiği (pcap uzantılı dosyaları) parse işlemine tabi tutarak kritik bilgileri bizim yerimize kendisi bulan bir araçtır. Şimdi az önce elle yaptığımız şifre bulma işini bu sefer Network Miner'a otomatize bir şekilde yaptıralım. Bu iş için ilk olarak Wireshark'tan elde edilen paketleri pcap uzantılı bir dosyaya toplamamız gerekmektedir. Fakat pcap dosyalamasını yapabilmek için önce Wireshark'ın paket sniff'leme işlemini kırmızı kareye tıklayarak durdurmamız gerekir.

| 8 🗆 🗉 | includekara | Differentiark 1.10.0 | 5 (v1.10.6 from master-1.1 | 0)] | |
|-----------|-------------------|--------------------------|----------------------------|--------------------|---|
| File Edi | t View Ge 🙆 | pture Analyze Statistics | Telephony Tools Internals | Help | |
| • | | 🛃 🛅 🛅 🗶 🦿 | Q < > 🕉 | ¥ 🖌 🗐 | |
| Filte Sto | p the running liv | ve capture | ▼ Expressio | n Clear App | ply Save |
| No. | Time | Source | Destination | Protocol Leng | gtł Info |
| 1679 | 243.22251000 | 192.168.0.12 | 93.89.224.247 | тср | 54 [TCP Keep-Alive] 49853 > http [ACK] Seq=1573 Ack=3 |
| 1680 | 243.28613800 | 93.89.224.247 | 192.168.0.12 | ТСР | 60 [TCP Keep-Alive ACK] http > 49853 [ACK] Seq=3416 A |
| 1681 | 246.30768800 | 172.217.16.99 | 192.168.0.12 | TLSv1.2 | 109 Application Data |
| 1682 | 246.30772900 | 9 192.168.0.12 | 172.217.16.99 | TCP | 54 34525 > https [ACK] Seq=446 Ack=4608 Win=40832 Len |
| 1683 | 246.30773600 | 172.217.16.99 | 192,168,0,12 | TCP | 60 https > 34525 [FIN, ACK] Seg=4608 Ack=446 Win=9011 |

Şimdi File -> Save As diyerek ekrana gelen penceredeki dosya uzantısı kısmına Wireshark/tcpdump – pcap diyelim ve isim olarak da örneğin includekarabuk demiş olalım.

| ve in folder: | home hefese | | Create Fold |
|---------------|-------------------------|--------------------------|--------------------|
| Places | Name | Size | Modified |
| ft Home | Android | | 15-09-2015 |
| Desktop | 🚞 android-studio | | 19-08-2015 |
| befese | 📄 AndroidStudioProjects | | 17-12-2015 |
| Therese | arachni-1.4-0.5.10 | | 09-02-2016 |
| Devices | backports-3.16-1 | | 30-04-2016 |
| Computer | CodeBlocksProjects | | 03-05-2016 |
| S D4D8-1 ▲ | crunch-3.4 | | 19-01-2016 |
| 🖪 TOSHIBA 🔺 | Desktop | | 09:09 |
| | Documents | | 05-04-2016 |
| | Downloads | | Yesterday at 01:29 |
| | 📄 dwhelper | | 30-04-2016 |
| | EclipseProjects | | 07-09-2014 |
| | genymotion | | 30-09-2015 |
| | bashcat-2 00 | | 29-02-2016 |

Save diyerek pcap dosyasını oluşturalım. Dosya oluştuktan sonra sırada dosyayı Network Miner'a vermek vardır. Önce NetworkMiner'ı kuralım.

- > sudo apt-get install libmono-winforms2.0-cil
- > wget www.netresec.com/?download=NetworkMiner -O /tmp/nm.zip
- > sudo unzip /tmp/nm.zip -d /opt/
- > cd /opt/NetworkMiner*
- > sudo chmod +x NetworkMiner.exe
- > sudo chmod -R go+w AssembledFiles/
- > sudo chmod -R go+w Captures/
- > mono NetworkMiner.exe

NOT: Eğer program zaten kuruluysa programı başlatmak için şu iki satırı girmen yeterli:

> cd /opt/NetworkMiner*
> mono NetworkMiner.exe

NetworkMiner programı başladığında karşımıza aşağıdaki ekran gelecektir:

| NetworkMiner 2.0 | |
|--|-------------------|
| File Tools Help | |
| | Case Panel |
| Hosts Files Images Messages Credentials Sessions DNS Parameters Keywords Anomalies | File MD5 |
| Sort Hosts On: IP Address (ascending) Sort and Refresh | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | 1 |
| 1 | Reload Case Files |
| Running NetworkMiner with Mono | |

Şimdi Wireshark'tan elde ettiğimiz pcap dosyasını NetworkMiner'a verelim.





Pcap dosyası aşağıdaki gibi NetworkMiner'a yüklenecektir.



| 😣 🗖 🗊 NetworkMiner 2.0 | _ |
|--|--------------------|
| File Tools Help | |
| Keywords Anomalies | Case Panel |
| Hosts (91) Files (127) Images (6) Messages Credentials (1) Sessions (60) DNS (197) Parameter | Filename MD5 |
| ♥ Show Cookies ♥ Show NTLM challenge-response | includekarab 29ac2 |
| Client Server | |
| 192.168.0.12 [HEFESE-N61JQ] 54.235.146.142 [engine3-774595980.us-east-1.elb.amazonaws.com] | |
| 192.168.0.12 [HEFESE-N61JQ] 151.101.65.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchar | |
| 192.168.0.12 [HEFESE-N61JQ] 151.101.65.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchar | |
| 192.168.0.12 [HEFESE-N61JQ] 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchang | |
| 192.168.0.12 [HEFESE-N61JQ] 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchang | |
| 192.168.0.12 [HEFESE-N61JQ] 104.16.112.18 [stack.imgur.com.cdn.cloudflare.net] [i.stack.imgur.co | |
| 192.168.0.12 [HEFESE-N61JQ] 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchang | |
| 192.168.0.12 [HEFESE-N61JQ] 95.172.94.39 [anycast-europe.quantserve.com.akadns.net] [akamai- | |
| 192.168.0.12 [HEFESE-N61]Q] 93.89.224.247 [includekarabuk.com] [www.includekarabuk.com] | |
| 192.168.0.12 [HEFESE-NG1]Q] 80.239.149.17 [a1294.wz0.akamai.net] [b.scorecardresearch.com.ed | |
| 192.100.0.12 [HEFESE-N01]Q] 95.09.224.247 [includekalabuk.com] [www.includekalabuk.com] | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Ⅰ |
| ٩ | Reload Case Files |
| Running NetworkMiner with Mono | |

Pcap dosyası böylece NetworkMiner'a yüklenmiştir ve parse işlemi de son bulmuştur. Şimdi Credentials sekmesine geçelim.

| 😣 🖨 🗊 Network Miner 🕯 | 2.0 | | |
|-------------------------------|---|----------|------------|
| File Tools Help | | | |
| Keywords Anomalies | | Case Pan | el —— |
| Hosts (91) Files (127) Image | s (6) Messages Credentials (11) Sessions (60) DNS (197) Paramete | File | MD5 |
| Show Cookies 🔽 Show N | ITLM challenge-response 🗖 Mask Passwords | include | 29ac2 |
| Client | Server | | |
| 192.168.0.12 | 93.89.224.247 [includekarabuk.com] [www.includekarabuk.com] | | |
| 192.168.0.12 | 93.89.224.247 [includekarabuk.com] [www.includekarabuk.com] | | |
| 192.168.0.12 | 151.101.65.69 [askubuntu.com] | | |
| 192.168.0.12 | 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] | | |
| 192.168.0.12 | 104.16.112.18 [stack.imgur.com.cdn.cloudflare.net] [i.stack.imgur.com | | |
| 192.168.0.12 | 80.239.149.17 [a1294.w20.akamai.net] [b.scorecardresearch.com.edg | | |
| 192.168.0.12 | 95.172.94.39 [anycast-europe.quantserve.com.akadns.net] [akamai-pi: | | |
| 192.168.0.12 | 151.101.65.69 [askubuntu.com] [cdn.sstatic.net] | | |
| 192.168.0.12 | 54.235.146.142 [engine3-774595980.us-east-1.elb.amazonaws.com] [e | | |
| 192.168.0.12 | 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchange | | |
| 192.168.0.12 [HEFESE-N61JQ] | 151.101.1.69 [askubuntu.com] [cdn.sstatic.net] [area51.stackexchange | | |
| | I | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| • | <u>}</u> | Reload (| Case Files |
| Rupping NetworkMiner with Mor | | L | |

Görüldüğü üzere 11 tane credentials tespit edildiği gösterilmektedir. Bunlardan çoğu çerez olacağı için çerezleri ayıklayalım. Bunun için Show Cookies tick'ini kaldıralım.

| 😣 🖱 💷 NetworkMiner 2.0 | |
|--|--|
| File Tools Help | |
| Keywords Anomalies Hosts (91) Files (127) Images (6) Messages Credentials (1) Sessions (60) DNS (197) Parameter Show Cookles Show NTLM challenge-response Mask Passwords | Case Panel Filename MD5 includekarab 29ac2 |
| Client Server | |
| 192.168.0.12 [HEFESE-N61JQ] 93.89.224.247 [includekarabuk.com] [www.includekarabuk.com] 192.168.0.12 [HEFESE-N61JQ] 192.168.0.12 [HEFESE-N61JQ] | |
| | |
| Running NetworkMiner with Mono | .:: |

Geriye bir tane credential kalmıştır. İşte o bizim includekarabuk'ün admin paneline girerken POST ettiğimiz kullanıcı adını ve şifreyi tutan pakettir. Kullanıcı adı ve şifreyi çekmek için sırasıyla ilgili satıra sağ tıklayalım ve bir Copy Username diyelim, bir de Copy Password diyelim.

| 😣 🖻 💷 NetworkMiner 2.0 | | |
|--|-----------------------------------|-------------|
| File Tools Help | | |
| Keywords Anomalies Hosts (91) Files (127) Images (6) Messages Credentials (1) Show Cookies Show NTLM challenge-response Mask Passwords | e Panel M name M udekarab 2 | ID5 9ac2 |
| Client Server | | |
| 192.168.0.12 [HEFESE-N61JQ] 93.89.22 Copy Username Copy Password Auto-resize all columns | eload Case Fil | ► es |
| Running NetworkMiner with Mono | | |

| 😣 🖨 💷 NetworkMiner 2.0 | | |
|--|--------------|-------|
| File Tools Help | | |
| Keywords Anomalies | Case Panel — | |
| Hosts (91) Files (127) Images (6) Messages Credentials (1) Sessions (60) DNS (197) Paramete | Filename | MD5 |
| ☐ Show Cookies | includekarab | 29ac2 |
| Client Server | | |
| 192.168.0.12 [HEFESE-N61]Q] 93.89.224.247 [includ Copy Username Copy Password Auto-resize all columns | | Þ |
| | Reload Case | files |
| Running NetworkMiner with Mono | | .: |

Kopyaladıklarımızı sırasıyla bir metin belgesine yapıştırarak kullanıcı adı ve şifre bilgisine erişmiş oluruz. Sonuç olarak fark ettiysen Wireshark'ta kullanıcı adı ve şifreyi bulmak için onca paket yığını içerisinde boğuşuyorduk ve elimizle filtreler girerek sonuca ulaşmaya çalışıyorduk. NetworkMiner'da ise bu filtreleme işini bizim yerimize programın kendisi yapıyor ve şıp diye trafik içerisinde bulduğu kullanıcı adı ve şifreyi önümüze sunuyor.

NOT: NetworkMiner normalde bir Windows yazılımıdır ve ayrıca Windows'ta exe'si indirildiği takdirde bir kuruluma gerek kalmadan direk çift tıkla - çalıştır pratikliğindedir.