

```
Windows PowerShell + 
Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::ea72:bf1b:38c2:4b4b%7
  IPv4 Address . . . . . : 192.168.0.100
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

PS C:\WINDOWS\System32> arp -a

Interface: 192.168.0.100 --- 0x7
  Internet Address      Physical Address      Type
  192.168.0.1           60-83-e7-30-fa-1d    dynamic
  192.168.0.108         10-a5-1d-7f-93-ec    dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22             01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

PS C:\WINDOWS\System32>
```

```
Windows PowerShell + 
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\WINDOWS\System32> arp -a

Interface: 192.168.0.100 --- 0x7
  Internet Address      Physical Address      Type
  192.168.0.1           60-83-e7-30-fa-1d    dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22             01-00-5e-00-00-16    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

PS C:\WINDOWS\System32> ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::ea72:bf1b:38c2:4b4b%7
  IPv4 Address . . . . . : 192.168.0.100
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

PS C:\WINDOWS\System32> arp -a

Interface: 192.168.0.100 --- 0x7
  Internet Address      Physical Address      Type
  192.168.0.1           60-83-e7-30-fa-1d    dynamic
  192.168.0.100          192.168.0.100        static
  255.255.255.0          255.255.255.0        static
```

Host List x

IP Address	MAC Address	Description
192.168.0.100	60:83:E7:30:FD:1D	
192.168.0.100	50:C2:E8:D4:F2:FD	
192.168.0.101	64:0C:91:AB:5E:F9	
192.168.0.102	3C:E3:6B:C8:00:4E	

Ettercap
0.8.31(EB)

MITM menu

- ARP poisoning...
- NDP poisoning
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- Stop MITM attack(s)
- SSL Intercept

Delete Host Add to Target1 Add to Target2

DHCP:[50:C2:E8:D4:F2:FD] REQUEST 192.168.0.100
Randomizing 255 hosts for scanning...
Randomizing 255 hosts for 255 hosts...
4 hosts added to the host list
Host 192.168.0.100 added to TARGET1
Host 192.168.0.1 added to TARGET2

Capturing from wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2194	6.03366558	44.228.249.3	192.168.0.100	HTTP	1161	HTTP/1.1 200 OK (text/html)
4845	32.637982329	192.168.0.100	44.228.249.3	HTTP	725	[TCP ACKed unseen segment] [TCP Previous segment not captured] POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
5448	33.507423444	44.228.249.3	192.168.0.100	HTTP	57	HTTP/1.1 200 OK (text/html)

```
document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }]\nelse if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();\n}\nMM_reloadPage(true);\n/\n</script>\n</head>\n</html>\n</div>\n<div id="mainLayer" style="position:absolute; width:700px; z-index:1">\n<div id="mastehead">\n<h1 id="siteName">a href="https://www.acunetix.com/"\n<div id="mahaNav">\n<table border="0" cellpadding="0" cellspacing="0" width="100%">\n<tr>\n<td align="left">\n<div style="float:left; margin-right:10px">\n<a href="#">Home</a>\n<a href="#">Categories</a> | <a href="#">Artists</a> | <a href="#">Albums</a> | \n<a href="#">Guestbook</a> | <a href="#">Cart</a> | \n<a href="#">AJAX Demo</a>\n</div>\n<div style="float:left; margin-right:10px">\n<img alt="right" style="vertical-align:middle; margin-right:5px"/>\n<div style="display:inline-block; vertical-align:middle; font-size:small; padding:0 5px">\n</div>\n</div>\n</td>\n</tr>\n</table>\n</div>\n</div>
```

Packet (161 bytes) Reassembled TCP (2595 bytes) De-chunked entity body (2195 bytes) Uncompressed entity body (4958 bytes)

Packet 18620 - Displayed: 3 (0.0%) Profile: Default

The figure shows a screenshot of NetworkMiner, a network traffic analysis tool. The interface is divided into several panes:

- Top Bar:** Capturing from wlan0, File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Left Sidebar:** Shows tabs for http, https, dns, and others.
- Session List:** Shows a list of captured sessions with details like Source IP, Destination IP, Protocol, Length, and Info.
- Selected Session Content:** A large pane showing the raw and de-chunked entity body of a selected session. It includes code snippets for JavaScript and PHP, and detailed HTTP headers.
- Bottom Status Bar:** Displays packet count, reassembled bytes, de-chunked bytes, uncompress bytes, and profile information.

