

# Tracking Down the Phantom Host

John Payton 2003-06-18

## Tracking Down the Phantom Host

by John Payton

last updated June 18, 2003

Most information systems security professionals are familiar with the procedures for identifying malicious traffic among their routine data, and many of the same professionals are familiar with the forensic procedures required once you have identified a compromised host. But on more than one occasion, I have been asked how to locate a problem host when you are not sure where it is physically located.

This problem can arise innocently, such as when network wiring diagrams are not kept up-to-date, or not-so-innocently, when the less-than-trustworthy administrator decides to put a web server on the company's DMZ so as not to use all the available bandwidth on his home cable modem. Let's suppose this is the case, and you start seeing that server probing port 80 on other machines attached to your network. You dump the traffic, and the request it is making looks a little something like this:

```
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
%u9090%u6858%ucbd3
%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u81
90%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

...and you think, "OK, I have the IP address of the machine that is trying to infect my network with CodeRed, but where do I go from here?"

Relax. In the former case, it is relatively easy to locate the machine if you know the IP address. In the case of the ethics-challenged admin, however, it can be quite difficult to locate the offending host, as the owner of the system likely does not want it found. There are examples ranging from hidden hosts above the ceiling tiles and below the raised floor, to rogue servers installed in elevator shafts and wired (rather professionally) into the facility cable plant.

### The Easy Way

The easiest way to go about finding the host is to ping the IP address that is performing the offending action (be that hogging precious network bandwidth, or providing IRC connectivity to burgeoning

h4x0rs). This is assuming that you have a relatively small network, that your interest was piqued while you were located on the local segment with the host, and assuming that it has not been hardened in an attempt to protect its secret location. Check the Time-To-Live (TTL) to verify that the rogue host is on the same segment. If you are on the same broadcast domain, the TTLs should not decrement. They should be 255, 128, 64, or 32. I can think of only a couple of instances where they will not be one of these numbers.

```
C:\>ping 10.1.1.100
```

```
Pinging 10.1.1.10 with 32 bytes of data:
```

```
Reply from 10.1.1.100: bytes=32 time<1ms TTL=128
```

```
Reply from 10.1.1.100: bytes=32 time<1ms TTL=128
```

```
Reply from 10.1.1.100: bytes=32 time<1ms TTL=128
```

```
Reply from 10.1.1.100: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.1.1.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If it is not on the same logical segment, use traceroute to determine hop count and identify the segment you should be on to locate the host. Use the command `tracert` in Windows and `traceroute` in Linux or Unix.

```
C:\>tracert 172.16.1.100
```

```
Tracing route to 172.16.1.100 over a maximum of 30 hops
```

1	*	*	*	Request timed out.
2	1 ms	1 ms	1 ms	10.1.1.1
3	13 ms	13 ms	11 ms	172.16.1.254
4	11 ms	11 ms	11 ms	172.16.1.100

```
Trace complete.
```

Bear in mind that being on the same logical segment simply means you do not have a router or other

device that will decrement the TTL between you and the host in question. You may still have a Layer 2 device to traverse before you are on the same physical segment with your host. Once you have determined the physical segment and have situated yourself accordingly, ping and check your ARP cache.

Remember, the Internet Protocol [1] is a layer 3 protocol and knows nothing about the hardware associated with the assigned IP address. To find the physical address of the destination host, the Address Resolution Protocol (ARP)[2] is used to locate the host. Notice in the example below that the ARP cache shows no entry for 10.1.1.180. Once a ping is initiated, the Address Resolution Protocol sends a broadcast to the local segment looking for the hardware address associated with that IP address. Checking the ARP cache again will display the entry for 10.1.1.180.

From Windows:

```
C:\>arp -a
```

```
Interface: 10.1.1.160 --- 0x2
```

Internet Address	Physical Address	Type
10.1.1.130	00-60-cf-20-b3-72	dynamic
10.1.1.132	00-90-27-d0-8a-07	dynamic
10.1.1.133	00-06-5b-3d-16-32	dynamic
10.1.1.254	08-00-20-c3-9a-9e	dynamic

```
C:\>ping 10.1.1.180
```

```
Pinging 10.1.1.180 with 32 bytes of data:
```

```
Reply from 10.1.1.180: bytes=32 time<1ms TTL=255
```

```
Reply from 10.1.1.180: bytes=32 time<1ms TTL=255
```

```
Reply from 10.1.1.180: bytes=32 time<1ms TTL=255
```

```
Reply from 10.1.1.180: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 10.1.1.180:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>arp -a
```

```
Interface: 10.1.1.160 --- 0x2
```

Internet Address	Physical Address	Type
10.1.1.130	00-60-cf-20-b3-72	dynamic
10.1.1.132	00-90-27-d0-8a-07	dynamic
10.1.1.133	00-06-5b-3d-16-32	dynamic
10.1.1.180	08-00-20-fd-c6-52	dynamic
10.1.1.254	08-00-20-c3-9a-9e	dynamic

From Linux the output will look a little different:

```
[root@portcullis root]# arp -a
www.testlan.xyz (10.1.1.130) at 00:60:cf:20:b3:72 [ether] on eth0
dns.testlan.xyz (10.1.1.100) at 00:90:27:d0:8a:07 [ether] on eth0
mail.testlan.xyz      (10.1.1.200) at 08:00:20:c3:9a:9e [ether] on eth0
```

But the information is still the same. All together, this a relatively easy way to come up with the hardware address associated with your rogue IP. It will not always be that easy.

## The Hard Way

In the event the perpetrator of this heinous theft of network resources has taken steps to mask his illicit activity from view, and is offering a only single service on the machine, and will not accept connections to any other ports, the task can get much harder. The ping test will not work. And as such, you will have to find other means of locating the box. Much has been written on identifying the service being offered by banner grabbing and identifying the OS by passive fingerprinting. I won't belabor those topics by rehashing them here, much more thorough research than mine has been done on the subject. Toby Miller has written a couple of excellent papers on the subject, which can be found at [\[3\]](#) and [\[4\]](#). Just be cognizant of the fact that it may be a little harder to originally identify the MAC address. You may have to capture the traffic to find the MAC address for the end hop of the segment you are currently monitoring and then, hop-by-hop, trace it back to its origin.

## Either Way

Once you have the MAC address, you can login to your switch and begin to track down the host. Again, unless you are on the same segment as the host in question, you are tracking down one leg in the journey to the destination.

Once you are logged into the switch, the command `show cam dynamic` will show the dynamic entries in

the Content-Addressable Memory (CAM) table on a Cisco CatOS switch [5]. More specifically, it will show you the mapping of hardware addresses to switch ports. For switches with the CatIOS, the command would be `show mac`.

Cisco Systems Console

Enter password:

Console> show cam dynamic

\*=Static Entry. +=Permanent Entry. #=System Entry. R=Router Entry.

X=Port Security Entry \$=Dot1x Security Entry

VLAN Dest MAC/Route Des [CoS] Destination Ports or VCs/ [Protocol Type]

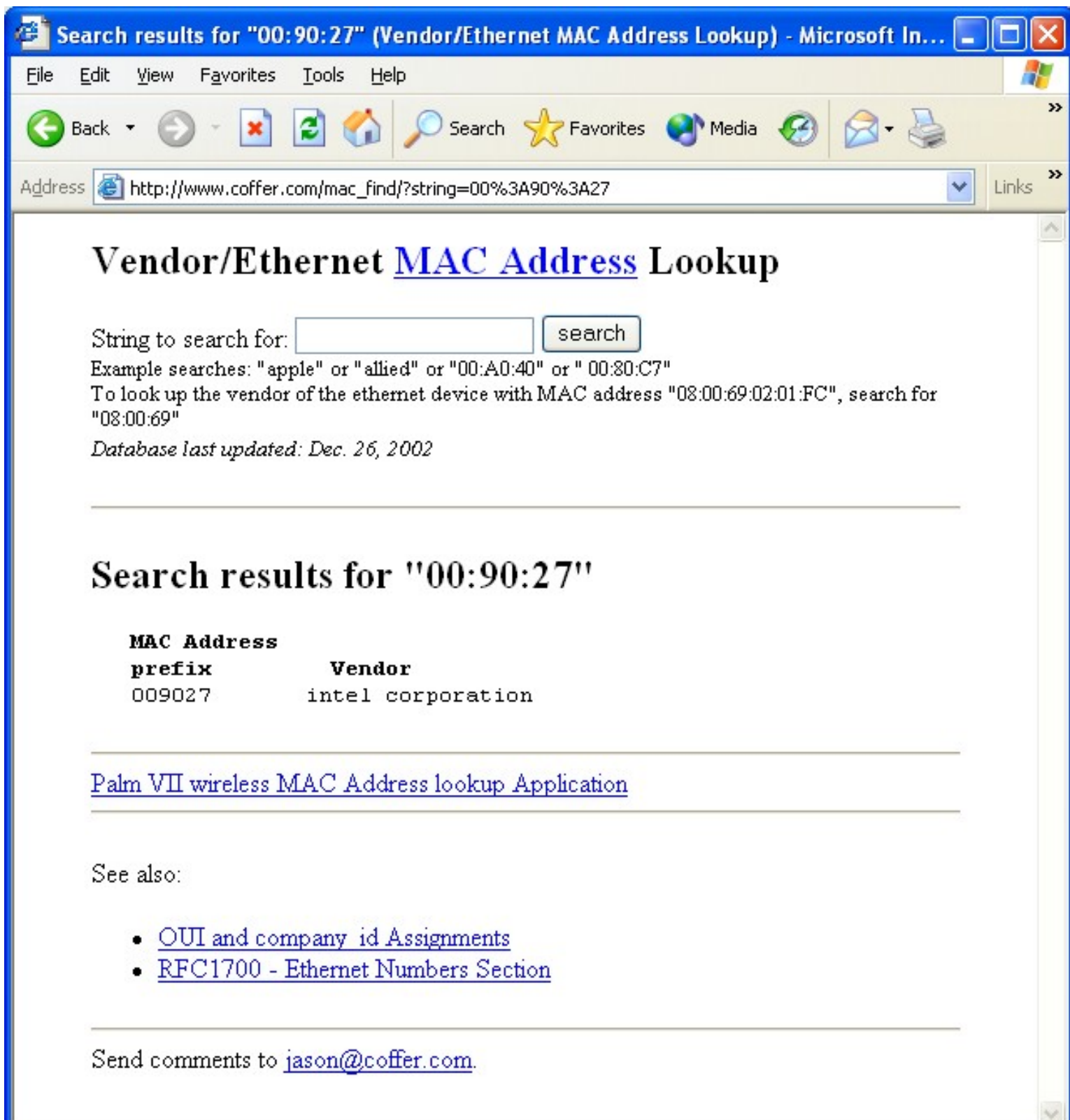
```
-----
592  00-b0-d0-ab-b7-40          3/15 [ALL]
590  00-b0-d0-ea-38-fc          4/16 [ALL]
592  00-04-75-c1-a2-6e          3/39 [ALL]
592  00-06-5b-3d-16-32          3/31 [ALL]
590  00-b0-d0-ea-3e-c4          4/16 [ALL]
590  00-b0-d0-fc-45-3d          3/37 [ALL]
590  08-00-20-e7-64-87          3/41 [ALL]
590  08-00-20-bf-b4-a2          3/48 [ALL]
590  00-06-2a-f9-03-04          4/13 [ALL]
592  08-00-20-c3-9a-9e          3/35 [ALL]
590  00-06-5b-84-28-34          4/13 [ALL]
592  02-01-00-00-00-01          4/7  [ALL]
590  00-b0-d0-ea-2a-ea          4/16 [ALL]
590  00-b0-d0-ea-2a-5e          4/16 [ALL]
592  00-01-02-6c-f4-58          3/45 [ALL]
592  00-01-02-6c-f4-48          4/3  [ALL]
592  00-01-02-6c-f4-d9          3/26 [ALL]
592  00-90-27-d0-8a-07          3/28 [ALL]
592  00-04-75-96-d8-35          4/6  [ALL]
592  00-04-75-96-d8-7d          3/22 [ALL]
592  00-04-75-96-d8-dc          3/5  [ALL]
592  00-04-75-96-d7-7b          4/6  [ALL]
```

Do you wish to continue y/n [n]? y

Armed with the knowledge of the module and port number, we can proceed to trace the connection to

the host. There is a possibility that the cable you trace from the port may lead to another segment and you will have to start this procedure again from the beginning.

This would also be a good time to look up the MAC address by vendor. One place to perform said lookup is located at [http://www.coffer.com/mac\\_find/](http://www.coffer.com/mac_find/). Another is <http://standards.ieee.org/regauth/oui/index.shtml>. The former, in my humble opinion, is better for looking up the address itself, and the latter is better for looking up the address ranges assigned to a particular vendor. But to each his own.



The screenshot shows a Microsoft Internet Explorer browser window with the title "Search results for '00:90:27' (Vendor/Ethernet MAC Address Lookup) - Microsoft In...". The address bar contains the URL [http://www.coffer.com/mac\\_find/?string=00%3A90%3A27](http://www.coffer.com/mac_find/?string=00%3A90%3A27). The main content area displays the heading "Vendor/Ethernet MAC Address Lookup". Below this is a search form with a text input field containing "00:90:27" and a "search" button. Example searches are listed: "apple" or "allied" or "00:A0:40" or "00:80:C7". A note states: "To look up the vendor of the ethernet device with MAC address '08:00:69:02:01:FC', search for '08:00:69'". The database is noted as last updated on Dec. 26, 2002. The search results are presented in a table:

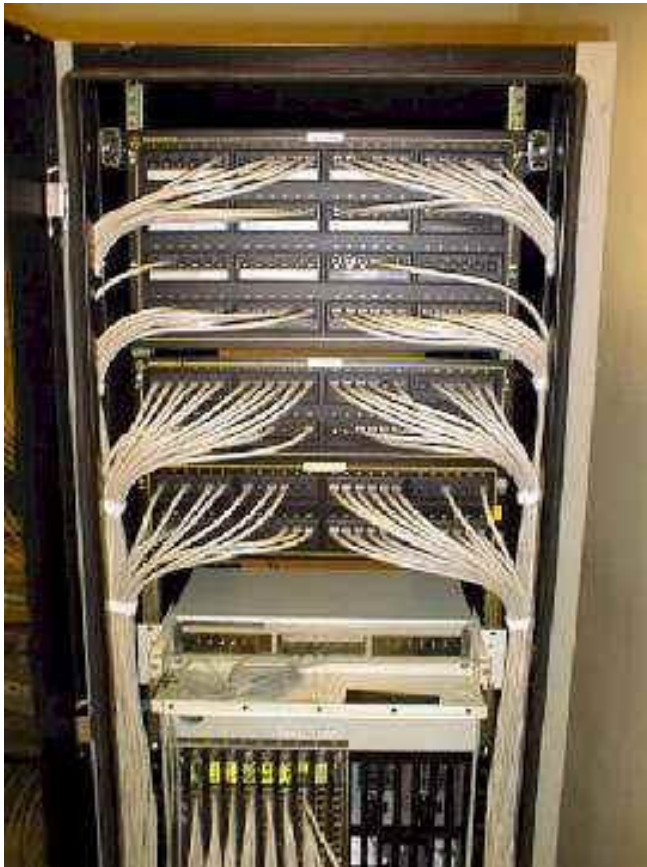
MAC Address prefix	Vendor
009027	intel corporation

Below the table is a link to "Palm VII wireless MAC Address lookup Application". A "See also:" section contains two links: "OUI and company id Assignments" and "RFC1700 - Ethernet Numbers Section". At the bottom, there is a link to "Send comments to [jason@coffer.com](mailto:jason@coffer.com)".



This lookup won't necessarily tell you everything about the host you're looking for, but it can definitely help to narrow the field by telling you the NIC vendor or telling you the vendor of the hardware in question. It can also serve to inform you as to your proximity (or lack thereof) to the host. For example, if the MAC lookup turns up a listing for Cisco Systems, and the host you're looking for is running Apache on Linux, you can probably continue your search and take comfort in the knowledge that, while you have not found the interloping host, you are one step closer to your destination.

Once completed, all that remains is the trace to the host. This can be a tricky proposition at times, as the cable may run through the center of a bundle, or through cable trays above the ceiling tiles or below the floor.



There are a couple of other instances that are worth mentioning when considering the problem of rogue hosts. One is the rogue DHCP server, the other is a rogue wireless access point.

In the case of the rogue DHCP server, it can become a problem if it is offering IPs to all requests and has not been configured in accordance with local policy. Whereas a DHCP server can be used to set the default gateway and DNS servers used, a rogue DHCP server could be used to reroute traffic through a

false gateway, thereby making all traffic subject to sniffing or man-in-the-middle attacks. Procedures for locating a rogue DHCP server are the same as what has been detailed herein. All that remains is to see if the server will assign you an address (in Windows try `ipconfig /renew`) and then looking to see which DHCP server assigned the address (`ipconfig /all`).

Rogue wireless access points are a fairly recent problem. With the advent of 802.11, wireless networks are springing up everywhere. If you would like to identify any rogue APs in your network, I would recommend downloading a wireless sniffer and performing a "wardrive" against your network. For further information look here [6]. Once you have captured some traffic, check for default configurations.

A short list:

Vendor	Default SSID	Possible MAC	Default Channel(s)
3com	comcomcom		
Compaq	Compaq		
Cisco	tsunami, Wavelan Network		2, 3
D-Link	WLAN		11
Intel	101, 195, xlan, intel	00:A0:F8	
Linksys	linksys		3, 6, 11
Netgear	Wireless	00:30:AB	6
SMC	WLAN, BRIDGE	00:90:D1	11

An alternative way of going about it is to browse the CAM table looking for MAC address ranges belonging to popular wireless AP vendors.

## Parting Ways

When I originally started writing this article, I wrote it from the perspective of finding an unauthorized gaming server on your network and tracking it down. It was brought to my attention that a gaming server is not really a security risk. While it may be true that a gaming server is not, in and of itself, a security risk, I would submit that a rogue server whatever the function is a risk to your network's security. Information security is not about risk elimination, it is about risk acceptance. It is mostly impossible to eliminate all risk, therefore, we as security professionals perform analyses of the risk and help business units define acceptable levels of risk that still maintain functionality required to do business. Any unauthorized host has bypassed this risk analysis, and therefore, any risk it presents has not been accepted by management. Hopefully the procedures detailed in this article will help you find

and eliminate any unauthorized hosts on your networks.

The author would like to thank Hal Munsell, CCIE for originally teaching me this procedure.

*John Payton is an information systems security consultant in the Washington D.C. metropolitan area.*

---

## Relevant Links

- [1] RFC 791 - Internet Protocol
- [2] RFC 826 - An Ethernet Address Resolution Protocol
- [3] Miller, Toby (2001) [Passive OS Fingerprinting: Details and Techniques](#)
- [4] Miller, Toby (2003) [Passive OS Fingerprinting: Details and Techniques \(Part 2\)](#)
- [5] Rossi, Louis R. (2000) Cisco Catalyst LAN Switching, pg. 247-249
- [6] Phifer, Lisa (Apr 2003) [Sniffing the Air for Trouble](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus