## Using Wireshark: Identifying Hosts and Users

(<https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/>)

When a host is infected or otherwise compromised, security professionals need to quickly review packet captures (pcaps) of suspicious network traffic to identify affected hosts and users.

This tutorial offers tips on how to gather that pcap data using Wireshark, the widely used network protocol analysis tool. It assumes you understand network traffic fundamentals and will use [these](https://www.malware-traffic-analysis.net/training/host-and-user-ID.html) pcaps of [IPv4](https://en.wikipedia.org/wiki/IPv4) traffic to cover retrieval of four types of data:

* Host information from DHCP traffic
* Host information from NetBIOS Name Service (NBNS) traffic
* Device models and operating systems from HTTP traffic
* Windows user account from Kerberos traffic

Host Information from DHCP Traffic

Any host generating traffic within your network should have three identifiers: a [MAC address](https://en.wikipedia.org/wiki/MAC_address), an [IP address](https://en.wikipedia.org/wiki/IP_address), and a [hostname](https://en.wikipedia.org/wiki/Hostname).

In most cases, alerts for suspicious activity are based on IP addresses. If you have access to full packet capture of your network traffic, a pcap retrieved on an internal IP address should reveal an associated MAC address and hostname.

How do we find such host information using Wireshark? We filter on two types of activity: [DHCP](https://wiki.wireshark.org/DHCP) or [NBNS](https://wiki.wireshark.org/NetBIOS/NBNS). DHCP traffic can help identify hosts for almost any type of computer connected to your network. NBNS traffic is generated primarily by computers running Microsoft Windows or Apple hosts running MacOS.

The first pcap for this tutorial, ***host-and-user-ID-pcap-01.pcap***, is available in Canvas.

This pcap is for an internal IP address at 172.16.1.207. Open the pcap in Wireshark and add the ***DHCP*** filter. This filter should reveal all the DHCP traffic.

Select one of the frames that shows ***DHCP Request*** in the info column (Frame 45).

Go to the frame details section and expand the line for ***Dynamic Host Configuration Protocol (Request)***.

Expand the lines for ***Client Identifier*** and ***Host Name***.

Client Identifier details should reveal the MAC address assigned to 172.16.1.207, and Host Name details should reveal a hostname.

Looking through the DHCP section of this packet answer the following questions:

1. What is the Hostname for device 172.16.1.207?

Rogers-ipad

1. What is the MAC address for device 172.16.1.207?

7c:6d:62:d2:e3:4f

A MAC address is a long, Hexadecimal number that identifies both the manufacturer of a NIC as well as a unique ID (address) for that NIC.

1. If the MAC address is tied to the NIC of the device, who is the manufacturer of the NIC in frame you are analyzing?

Apple

1. What part of the MAC address is the Manufacturer ID part of the address?

7c:6d:62:

1. What part of the MAC address is the Unique ID part of the address?

D2:e3:4f

With the DHCP filter applied, you should only see frames that are part of a DHCP communication. Notice in the Info column that you see there are two different types of DHCP transactions: Request and ACK (stands for Acknowledge).

This is known as a Handshake sequence. Different protocols have different Handshake sequences. DHCP has a four-step handshake sequence.

* First – Discover a new machine on the network
* Second – Offer an available address
* Third – Request one of the available addresses
* Fourth – Ack – Acknowledge client’s request for address information.

Select one of the DHCP Request frames and answer the following:

1. What device is issuing IP addresses on this network (DHCP server)?

Rogers-iPad

1. What parameters is the device requesting from the DHCP server? (HINT: there are seven of them)

Subnet Mask, Classless Static Route, Router, Domain Name server, domain name, domain search, private/proxy auto discovery.

Select one of the DHCP ACK frames and answer the following questions:

1. How long is the DHCP lease going to last?

7 days

1. Can you determine the name of the Domain that these devices are part of?

Mshome.net

Host Information from NBNS Traffic

Depending on how frequently a DHCP lease is renewed, you might not have DHCP traffic in your pcap. Fortunately, we can use NBNS traffic to identify hostnames for computers running Microsoft Windows or Apple hosts running MacOS.

The second pcap for this tutorial, ***host-and-user-ID-pcap-02.pcap***, is available in Canvas.

This pcap is from a Windows host using an internal IP address at 10.2.4.101.

Open the pcap in Wireshark and filter on ***nbns***. This should reveal the NBNS traffic.

Select the first frame (Frame #5), and you can quickly correlate the IP address with a MAC address and hostname.

You will notice that in the middle pane, Wireshark has organized the information based on the different protocols included in the frame. You can also see a list of the protocols included in the frame stored inside the Frame section of the middle pane.

Open the Frame section of the pane and find the list of “Protocols in frame”. Note that this list matches the different sections shown in the middle pane

1. What are the protocols useded in Frame #5?

Eth:ethertype:Ip:udp: nbns

1. What is the IP address of the source machine (the one sending the frame)?

10.2.4.101

1. What is the MAC address of the source machine?

00:01:e6:69:53:5a

1. Who is the Manufacturer of the NIC?

HewlettP

1. What is the Host-name of the source machine?

Martin-win

1. What is the IP address of the destination machine (the one receiving the frame)?

10.2.4.1

1. What is the MAC address of the destination machine?

20:e5:2a:b6:93:f1

1. Who is the Manufacturer of the destination machine’s NIC?

Netgear

Device Models and Operating Systems from HTTP Traffic

User-agent strings from headers in HTTP traffic can reveal the operating system.

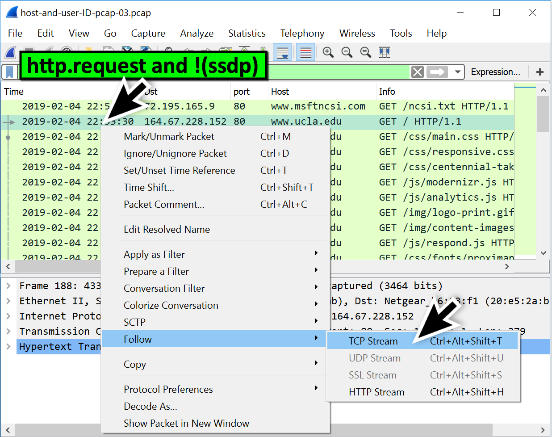
If the HTTP traffic is from an Android device, you might also determine the manufacturer and model of the device.

The third pcap for this tutorial, ***host-and-user-ID-pcap-03.pcap***, is available in Canvas.

This pcap is from a Windows host using an internal IP address at 192.168.1.97.

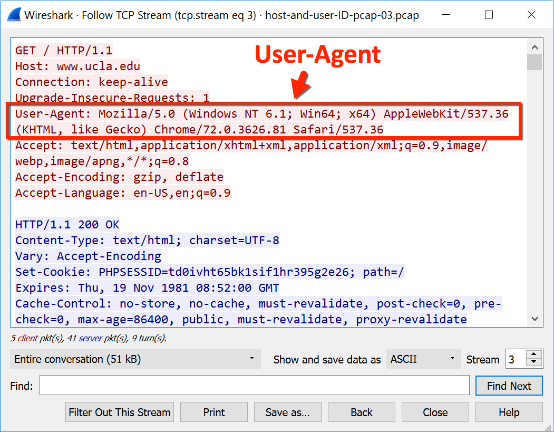
Open the pcap in Wireshark and filter on ***http.request and !(ssdp)***.

Select the second frame, which is the first HTTP request to ***www.ucla.edu***, and follow the TCP stream as shown in Figure 7.

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-7-Following-the-TCP-stream-for-an-HTTP-request-in-the-third-pcap..png)

*Figure 7: Following the TCP stream for an HTTP request in the third pcap*

This TCP stream has HTTP request headers as shown in Figure 8. The User-Agent line represents Google Chrome web browser version 72.0.3626[.]81 running on Microsoft’s Windows 7 x64 operating system.

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-8-The-User-Agent-line-for-a-Windows-7-x64-host-using-Google-Chrome..png)

*Figure 8: The User-Agent line for a Windows 7 x64 host using Google Chrome*

*Note the following string in the User-Agent line from Figure 8:*

***(Windows NT 6.1; Win64; x64)***

***Windows NT 6.1*** represents Windows 7. For User-Agent lines, Windows NT strings represent the following versions of Microsoft Windows as shown below:

* Windows NT 5.1:***Windows XP***
* Windows NT 6.0: ***Windows Vista***
* Windows NT 6.1:***Windows 7***
* Windows NT 6.2:***Windows 8***
* Windows NT 6.3:***Windows 8.1***
* Windows NT 10.0:***Windows 10***

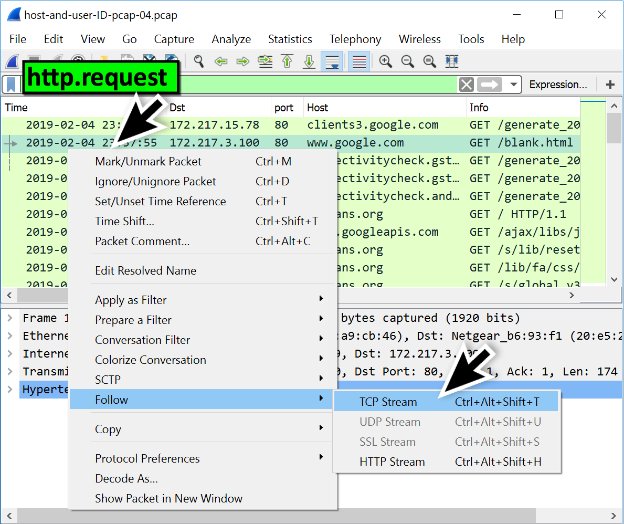
With HTTP-based web browsing traffic from a Windows host, you can determine the operating system and browser. The same type of traffic from Android devices can reveal the brand name and model of the device.

The fourth pcap for this tutorial, ***host-and-user-ID-pcap-04.pcap***, is available [here](https://www.malware-traffic-analysis.net/training/host-and-user-ID.html). This pcap is from an Android host using an internal IP address at 172.16.4.119. Open the pcap in Wireshark and filter on ***http.request***. Select the second frame in the list (Frame #107)

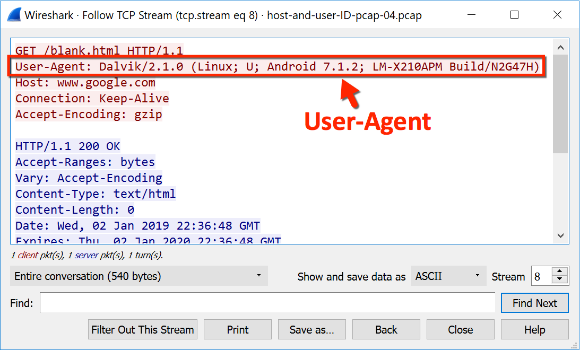
1. What webpage is being requested in this frame?

www.google.com/blank.html

Follow the TCP stream as shown in Figure 9.

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-9-Following-the-TCP-stream-for-an-HTTP-request-in-the-fourth-pcap..png)

*Figure 9: Following the TCP stream for an HTTP request in the fourth pcap*

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-10-The-User-Agent-line-for-an-Android-host-using-Google-Chrome..png)

*Figure 10: The User-Agent line for an Android host using Google Chrome*

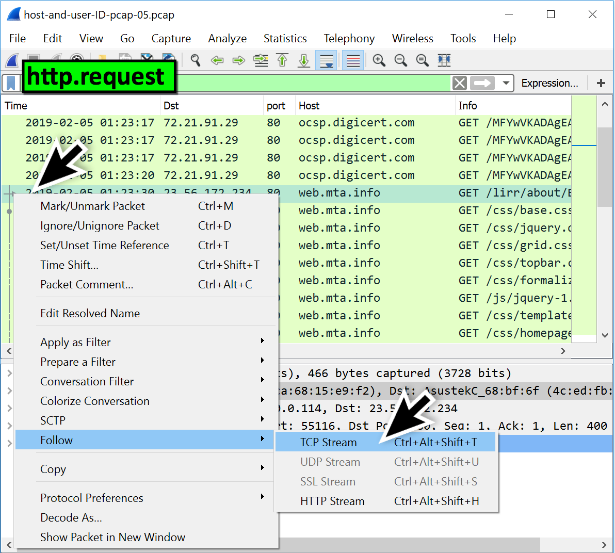
The User-Agent line in Figure 10 shows ***Android 7.1.2*** which is an older version of the Android operating system released in April 2017. ***LM-X210APM*** represents a model number for this Android device.

1. Can you figure out what type of phone was used to generate this traffic? (HINT: it used the above listed version of the Android Operating system and the aforementioned Android model device) (HINT #2: try using Google)

Nougat smartphone

The User-Agent line for HTTP traffic from an iPhone or other Apple mobile device will give you the operating system, and it will give you the type of device. However, it will not give you a model. We can only determine if the Apple device is an iPhone, iPad, or iPod. We cannot determine the model.

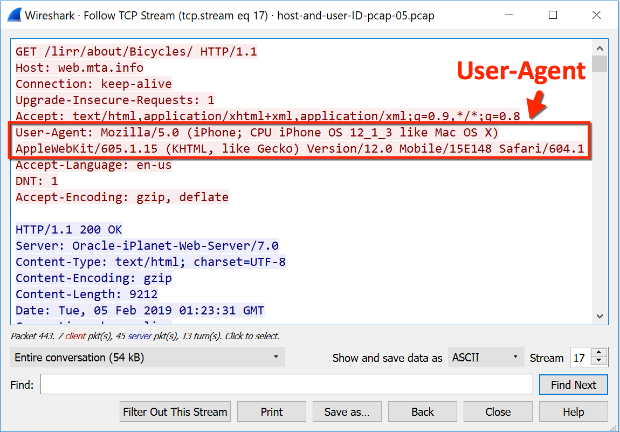
The fifth pcap for this tutorial, ***host-and-user-ID-pcap-05.pcap***, is available [here](https://www.malware-traffic-analysis.net/training/host-and-user-ID.html). This pcap is from an iPhone host using an internal IP address at 10.0.0[.]114. Open the pcap in Wireshark and filter on ***http.request***. Select the frame for the first HTTP request to ***web.mta[.]info***and follow the TCP stream as shown in Figure 11.

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-11-Following-the-TCP-stream-for-an-HTTP-request-in-the-fifth-pcap..png)

*Figure 11: Following the TCP stream for an HTTP request in the fifth pcap*

1. What phone and operating system generated this frame?

iphone: CPU iPhone OS 12\_1\_3 like Mac OS X) AppleWebKit/695.1.15

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-12-The-User-Agent-line-for-an-iPhone-using-Safari..png)

*Figure 12: The User-Agent line for an iPhone using Safari*

A final note about HTTP traffic and User-Agent strings: not all HTTP activity is web browsing traffic. Some HTTP requests will not reveal a browser or operating system. When you search through traffic to identify a host, you might have to try several different HTTP requests before finding web browser traffic.

Since more websites are using HTTPS, this method of host identification can be difficult. HTTP headers and content are not visible in HTTPS traffic. However, for those lucky enough to find HTTP web-browsing traffic during their investigation, this method can provide more information about a host.

Windows User Account from Kerberos Traffic

For Windows hosts in an Active Directory (AD) environment, we can find user account names in from Kerberos traffic.

The sixth pcap for this tutorial, ***host-and-user-ID-pcap-06.pcap***, is available [here](https://www.malware-traffic-analysis.net/training/host-and-user-ID.html). This pcap is from a Windows host in an Active Directory environment. (Hint: try looking in the CLDAP Protocol)

1. What is the name of the Windows Domain?

Happycraft.org

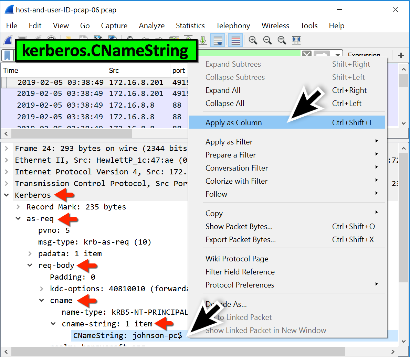
1. What is the name of the Server?

Johnson-pc

1. What is the name of the requesting PC?

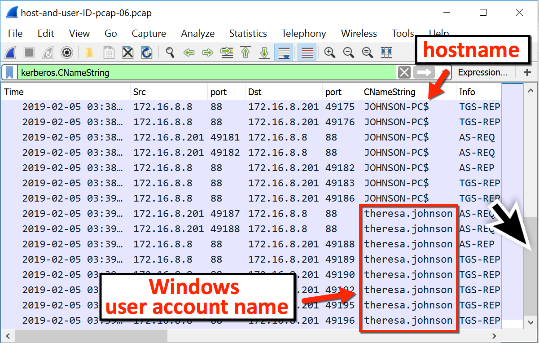
Dell

Open the pcap in Wireshark and filter on ***kerberos.CNameString***. Select the first frame. Go to the frame details section and expand lines as shown in Figure 13. Select the line with ***CNameString: johnson-pc$*** and apply it as a column.

[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-13-Finding-the-CNameString-value-and-applying-it-as-a-column..png)

*Figure 13: Finding the CNameString value and applying it as a column*

This should create a new column titled ***CNameString***. Scroll down to the last frames in the column display. You should find a user account name for ***theresa.johnson*** in traffic between the domain controller at 172.16.8[.]8 and the Windows client at 172.16.8[.]201 as shown in Figure 14.

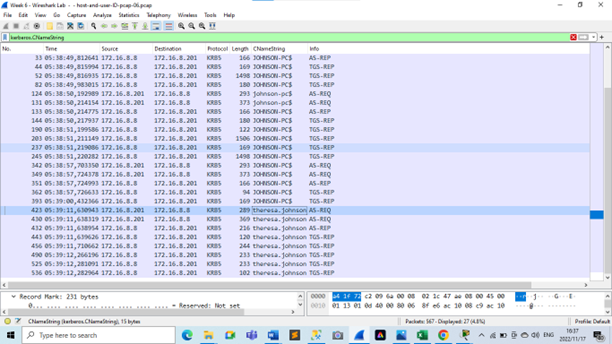
[](https://unit42.paloaltonetworks.com/wp-content/uploads/2020/03/Figure-14-Finding-the-W.png)

*Figure 14: Finding the Windows user account name*

CNameString values for hostnames always end with a ***$*** (dollar sign), while user account names do not. To filter on user account names, use the following Wireshark expression to eliminate CNameString results with a dollar sign:

***kerberos.CNameString and !(kerberos.CNameString contains $)***

1. Insert a screenshot of your Wireshark console showing the new column.



Summary

Proper identification of hosts and users from network traffic is essential when reporting malicious activity in your network. Using the methods from this tutorial, we can better utilize Wireshark to help us identify affected hosts and users.

Answer Sheet

Click or tap here to enter text.

Enter any content that you want to repeat, including other content controls. You can also insert this control around table rows in order to repeat parts of a table.