**Week 2 Lab Worksheet: Identifying Hosts, Devices, and Users**

Assignment: Week 2 Lab – Identifying Hosts and Users

Student: Lewis Joseph Feik
Date: January 21, 2026

## Part A — Open PCAP Files

- Opened 2022-MTA-workshop-macbook.pcap successfully in Wireshark (validated by packet parsing).
- Opened 2022-MTA-workshop-iPhone.pcap successfully in Wireshark (validated by packet parsing).
- Opened 2022-MTA-workshop-Android-phone.pcap successfully in Wireshark (validated by packet parsing).
- Opened 2022-MTA-workshop-Fedora-Linux.pcap successfully in Wireshark (validated by packet parsing).
- Opened 2022-MTA-workshop-Win11-host.pcap successfully in Wireshark (validated by packet parsing).

## Quick Summary (All PCAPs)

| PCAP / Device | Primary IP | Hostname (if visible) | Likely OS / Device |
|---|---|---|---|
| MacBook (2022-MTA-workshop-macbook.pcap) | 10.8.22.101 | Brad-MBP.local | macOS laptop (HTTP UA shows Mac OS X 10_15_7) |
| iPhone (2022-MTA-workshop-iPhone.pcap) | 10.8.21.213 | Home-iPhone | Apple iPhone (HTTP UA shows iPhone OS 15_6_1) |
| Android Phone (2022-MTA-workshop-Android-phone.pcap) | 172.16.1.121 | Galaxy-S20-FE-5G | Android phone (HTTP UA shows Android 12; Samsung SM-G781U) |
| Fedora Linux (2022-MTA-workshop-Fedora-Linux.pcap) | 10.8.30.128 | Not observed | Linux VM (Firefox on Linux; VMware MAC; Fedora DNS) |
| Windows 11 Host (2022-MTA-workshop-Win11-host.pcap) | 192.168.42.170 | DESKTOP-WIN11PC | Windows host (MSFT DHCP; TTL 128; Edge/NCSI UA) |

## PCAP 1: MacBook

File: 2022-MTA-workshop-macbook.pcap

### Part B — Host Identification

| Item | Value | Evidence (protocol / field) |
|---|---|---|
| Host IP address(es) | 10.8.22.101 | DHCP ACK (yiaddr) and observed IP traffic |
| Default gateway | 10.8.22.1 | DHCP option 3 (router) |

| | | |
|---|---|---|
| DHCP server | 10.8.22.1 | DHCP option 54 (server identifier) / ACK source |
| DNS server(s) | 10.8.22.1 | DHCP option 6 (DNS) |
| Hostname (if visible) | Brad-MBP.local | DHCP option 12; also LLMNR/NBNS/mDNS when present |
| Host MAC address | a4:83:e7:2a:45:d7 | Ethernet source MAC; DHCP chaddr |
| MAC vendor (if determinable) | Apple, Inc. | OUI prefix lookup (or MAC marked locally administered) |
| Gateway MAC address | 20:e5:2a:b6:93:f1 | ARP and Ethernet headers for gateway traffic |
| Gateway MAC vendor (if determinable) | NETGEAR | OUI prefix lookup (or MAC marked locally administered) |

- Hostnames also visible in NBNS queries: BRAD-MBP (NetBIOS Name Service).
- mDNS queries include Brad-MBP.local and services such as _airplay and _smb.

### Part C — OS & Device Indicators

- HTTP User-Agent observed (2 request(s)): Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.1 Safari/605.1.15 (HTTP).
- HTTP User-Agent observed (1 request(s)): CaptiveNetworkSupport-428.140.2 wispr (HTTP).
- Median IP TTL / Hop Limit from host traffic: 64 (IP header).
- Typical TCP SYN fingerprint: TTL=64, Window=65535, MSS=1460, WindowScale=6, SACK=True, Timestamps=True (TCP SYN options).
- DNS lookups include captive.apple.com and other Apple domains (DNS).
- mDNS service discovery includes Apple ecosystem services (mDNS).

### Part D — User Identification

- No explicit user account credentials or usernames were observed in clear text in this capture.
- Most application traffic is HTTPS/TLS encrypted, so user logins (usernames, emails, passwords) are typically not visible without endpoint logs or decrypted traffic.
- Sometimes a device name (hostname) can include a person's name (e.g., "Brad-MBP"), but that is a device label, not a verified user account.

## PCAP 2: iPhone

File: 2022-MTA-workshop-iPhone.pcap

## Part B — Host Identification

| Item | Value | Evidence (protocol / field) |
|---|---|---|
| Host IP address(es) | 10.8.21.213 | DHCP ACK (yiaddr) and observed IP traffic |
| Default gateway | 10.8.21.1 | DHCP option 3 (router) |
| DHCP server | 10.8.21.1 | DHCP option 54 (server identifier) / ACK source |
| DNS server(s) | 10.8.21.1 | DHCP option 6 (DNS) |
| Local domain (if any) | lan | DHCP option 15 (domain) |
| Hostname (if visible) | Home-iPhone | DHCP option 12; also LLMNR/NBNS/mDNS when present |
| Host MAC address | b0:ca:68:d9:19:82 | Ethernet source MAC; DHCP chaddr |
| MAC vendor (if determinable) | Apple, Inc. | OUI prefix lookup (or MAC marked locally administered) |
| Gateway MAC address | 20:e5:2a:b6:93:f1 | ARP and Ethernet headers for gateway traffic |
| Gateway MAC vendor (if determinable) | NETGEAR | OUI prefix lookup (or MAC marked locally administered) |

## Part C — OS & Device Indicators

- HTTP User-Agent observed (7 request(s)): com.apple.trustd/2.2 (HTTP).
- HTTP User-Agent observed (3 request(s)): Mozilla/5.0 (iPhone; CPU iPhone OS 15_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.1 Mobile/15E148 Safari/604.1 (HTTP).
- Median IP TTL / Hop Limit from host traffic: 64 (IP header).
- Typical TCP SYN fingerprint: TTL=64, Window=65535, MSS=1460, WindowScale=5, SACK=True, Timestamps=True (TCP SYN options).
- DNS lookups include Apple services (push / iCloud domains), consistent with iOS activity (DNS).

## Part D — User Identification

- No explicit user account credentials or usernames were observed in clear text in this capture.
- Most application traffic is HTTPS/TLS encrypted, so user logins (usernames, emails, passwords) are typically not visible without endpoint logs or decrypted traffic.
- Sometimes a device name (hostname) can include a person's name (e.g., "Brad-MBP"), but that is a device label, not a verified user account.

# PCAP 3: Android Phone

File: 2022-MTA-workshop-Android-phone.pcap

## Part B — Host Identification

| Item | Value | Evidence (protocol / field) |
|---|---|---|
| Host IP address(es) | 172.16.1.121, 2607:fb91:1201:4b3f:990a:8f60:f293:23fd, fe80::f09a:83ff:fe00:897d | DHCP ACK (yiaddr) and observed IP traffic |
| Default gateway | 172.16.1.1 | DHCP option 3 (router) |
| DHCP server | 172.16.1.1 | DHCP option 54 (server identifier) / ACK source |
| DNS server(s) | 172.16.1.1 | DHCP option 6 (DNS) |
| Hostname (if visible) | Galaxy-S20-FE-5G | DHCP option 12; also LLMNR/NBNS/mDNS when present |
| DHCP vendor class (if any) | android-dhcp-12 | DHCP option 60 (vendor class identifier) |
| Host MAC address | f2:9a:83:00:89:7d | Ethernet source MAC; DHCP chaddr |
| MAC vendor (if determinable) | Locally administered (randomized) – vendor not reliable from OUI | OUI prefix lookup (or MAC marked locally administered) |
| Gateway MAC address | 50:6a:03:bf:f6:57 | ARP and Ethernet headers for gateway traffic |
| Gateway MAC vendor (if determinable) | NETGEAR | OUI prefix lookup (or MAC marked locally administered) |

## Part C — OS & Device Indicators

- HTTP User-Agent observed (3 request(s)): Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36 (HTTP).
- HTTP User-Agent observed (2 request(s)): Mozilla/5.0 (Linux; Android 12; SAMSUNG SM-G781U) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/18.0 Chrome/99.0.4844.88 Mobile Safa… (HTTP).
- Median IP TTL / Hop Limit from host traffic: 64 (IP header).
- Typical TCP SYN fingerprint: TTL=64, Window=65535, MSS=1460, WindowScale=10, SACK=True, Timestamps=True (TCP SYN options).
- DHCP vendor class 'android-dhcp-12' and hostname 'Galaxy-S20-FE-5G' indicate an Android device (DHCP).
- DNS lookups include android.apis.google.com, play.google.com, and mtalk.google.com (DNS).
- The host MAC is locally administered (randomized), which is common on mobile devices for Wi-Fi privacy (Ethernet/DHCP).

## Part D — User Identification

- No explicit user account credentials or usernames were observed in clear text in this capture.
- Most application traffic is HTTPS/TLS encrypted, so user logins (usernames, emails, passwords) are typically not visible without endpoint logs or decrypted traffic.
- Sometimes a device name (hostname) can include a person's name (e.g., "Brad-MBP"), but that is a device label, not a verified user account.

## PCAP 4: Fedora Linux

File: 2022-MTA-workshop-Fedora-Linux.pcap

### Part B — Host Identification

| Item | Value | Evidence (protocol / field) |
|---|---|---|
| Host IP address(es) | 10.8.30.128 | DHCP ACK (yiaddr) and observed IP traffic |
| Default gateway | 10.8.30.2 | DHCP option 3 (router) |
| DHCP server | 10.8.30.254 | DHCP option 54 (server identifier) / ACK source |
| DNS server(s) | 10.8.30.2 | DHCP option 6 (DNS) |
| Local domain (if any) | localdomain | DHCP option 15 (domain) |
| Hostname (if visible) | Not observed | DHCP option 12; also LLMNR/NBNS/mDNS when present |
| Host MAC address | 00:0c:29:53:51:c0 | Ethernet source MAC; DHCP chaddr |
| MAC vendor (if determinable) | VMware, Inc. | OUI prefix lookup (or MAC marked locally administered) |
| Gateway MAC address | 00:50:56:ef:a7:3e | ARP and Ethernet headers for gateway traffic |
| Gateway MAC vendor (if determinable) | VMware, Inc. | OUI prefix lookup (or MAC marked locally administered) |

### Part C — OS & Device Indicators

- HTTP User-Agent observed (4 request(s)): Mozilla/5.0 (X11; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0 (HTTP).
- Median IP TTL / Hop Limit from host traffic: 64.0 (IP header).
- Typical TCP SYN fingerprint: TTL=64, Window=64240, MSS=1460, WindowScale=7, SACK=True, Timestamps=True (TCP SYN options).
- MAC OUI indicates VMware, suggesting the Linux host is running as a virtual machine (Ethernet).
- DNS lookups include fedoraproject.org and Firefox connectivity checks (DNS).

### Part D — User Identification

- No explicit user account credentials or usernames were observed in clear text in this capture.
- Most application traffic is HTTPS/TLS encrypted, so user logins (usernames, emails, passwords) are typically not visible without endpoint logs or decrypted traffic.
- Sometimes a device name (hostname) can include a person's name (e.g., "Brad-MBP"), but that is a device label, not a verified user account.

## PCAP 5: Windows 11 Host

File: 2022-MTA-workshop-Win11-host.pcap

### Part B — Host Identification

| Item | Value | Evidence (protocol / field) |
|---|---|---|
| Host IP address(es) | 192.168.42.170, 2600:100c:b01f:2102:2c20:ff1d:fb5:c3b, fe80::f5d4:82f0:5808:5db2 | DHCP ACK (yiaddr) and observed IP traffic |
| Default gateway | 192.168.42.129 | DHCP option 3 (router) |
| DHCP server | 192.168.42.129 | DHCP option 54 (server identifier) / ACK source |
| DNS server(s) | 192.168.42.129 | DHCP option 6 (DNS) |
| Hostname (if visible) | DESKTOP-WIN11PC | DHCP option 12; also LLMNR/NBNS/mDNS when present |
| DHCP vendor class (if any) | MSFT 5.0 | DHCP option 60 (vendor class identifier) |
| Host MAC address | 00:16:eb:f8:1c:c8 | Ethernet source MAC; DHCP chaddr |
| MAC vendor (if determinable) | Intel Corporate | OUI prefix lookup (or MAC marked locally administered) |
| Gateway MAC address | 62:35:18:bf:23:74 | ARP and Ethernet headers for gateway traffic |
| Gateway MAC vendor (if determinable) | Locally administered (randomized) – vendor not reliable from OUI | OUI prefix lookup (or MAC marked locally administered) |

- Hostnames also visible in LLMNR and NBNS: DESKTOP-WIN11PC and WORKGROUP.
- mDNS queries include DESKTOP-WIN11PC.local.

### Part C — OS & Device Indicators

- HTTP User-Agent observed (8 request(s)): Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 Edg/104.0.1293.70 (HTTP).
- HTTP User-Agent observed (2 request(s)): Microsoft NCSI (HTTP).
- Median IP TTL / Hop Limit from host traffic: 128.0 (IP header).
- Typical TCP SYN fingerprint: TTL=128, Window=64240, MSS=1460, WindowScale=8, SACK=True, Timestamps=False (TCP SYN options).
- DHCP vendor class 'MSFT 5.0' is typical of Windows DHCP clients (DHCP).
- DNS lookups include msftconnecttest.com and Windows Push Notification Service (DNS).
- LLMNR and NBNS name resolution traffic is consistent with Windows host behavior (LLMNR/NBNS).

### Part D — User Identification

- No explicit user account credentials or usernames were observed in clear text in this capture.

- Most application traffic is HTTPS/TLS encrypted, so user logins (usernames, emails, passwords) are typically not visible without endpoint logs or decrypted traffic.
- Sometimes a device name (hostname) can include a person's name (e.g., "Brad-MBP"), but that is a device label, not a verified user account.

## Part E — Analyst Reflection

Host and user identification matters because it turns "anonymous packets" into actionable context. Knowing which IP/MAC/hostname belongs to which device helps analysts build an asset inventory, detect rogue or unauthorized systems, prioritize alerts (for example, a domain controller versus a guest phone), and scope incidents faster. Even when user identities are not visible in traffic, documenting why (encryption, protocol choice, lack of authentication data) is part of a professional analysis and guides the next steps (endpoint logs, DHCP logs, authentication logs, or TLS decryption where authorized).

End of worksheet.