Packet Analysis

Analysing Network Traffic

Why Packet Analysis is Important

- Learn if someone (else) is sniffing a network
- Determine how port scanners and other tools work
- Identify malicious traffic
- Learn how malware works (calls home)
- Identifying bandwidth hogs
- Identifying network bottlenecks
- Performing intrusion detection and analysis
- Learning what attackers are doing

How to Capture Traffic

- Not just a matter of plugging an RJ45 cable into the network
- Different ways to capture traffic from a target device on a switched network
- Port mirroring
- Hubbing out (using a tap)
- ARP Poisoning
- ARP Flooding
- DHCP redirection

Promiscuous Mode

- A network card in promiscuous mode can receive all the data it can see, not just packets addressed to it
- By default, an Ethernet device only sees its own traffic. NIC drops packets not addressed to it
- In promiscuous mode NIC can capture frames from data-link layer right up to application layer
- WinPcap/LibPcap, (api) used to help applications such as Wireshark capture network traffic
- Summary
  - Promiscuous mode: captures all traffic the NIC can see
  - Non-promiscuous mode: captures only traffic addressed to it

Hubs and Switches

- Hubs are older, and quite rare these days
  - Broadcast devices

- Switches more common nowadays.

Hubbing out/Network Tap

- Hubs are basic, multiport repeater.
  - Traffic received in one port is broadcast out all other ports
  - Layer 1 device
  - Devices connected to a hub share same broadcast and collision domain
  - Low throughput (lots of collisions)
  - Great for network analysis
    - Anyone connected can see all traffic in that domain
  - Useful as a network tap

Switches

- Switches are considered intelligent devices
- Segment traffic by checking source and destination MAC addresses of each data frame
- Ability to learn which device is connected to each port of the switch
- As Ethernet frame comes in a port, the switch examines source MAC and compares it to what it has stored in memory
- This memory is known as a CAM Table (Content-Addressable Memory)
- CAM is RAM, holding a lookup table used to match each MAC address to the port it is connected to
- When data frame enters the switch, it finds the MAC address in the CAM table and matches it to the switch port
- Frame forwarded only to that port
- Layer 2 (sometimes also have functionality at layer 3)

Capturing Network Traffic

- To capture traffic, you must be on your local network
  - Connected to a hub, switch, router through which traffic passes
- **Passive sniffing** easy on a hub, as it broadcasts traffic
- When connecting on a switch, you have to take action to make the switch redirect traffic to you
- Active Sniffing, allows you to see traffic not addressed to you.
  - Port mirroring on a managed switch
  - ARP cache poisoning
  - Flooding
  - DHCP redirection
  - Redirection and interception with ICMP

Managed and Unmanaged Switches

- Unmanaged switch is basic plug and play device
- Managed devices have greater functionality
  - More expensive
    - Setting priority of service
    - Configuring VLANs
    - Using SNMP
    - Port mirroring
    - Spanning Tree (stops loops)

Port Mirroring

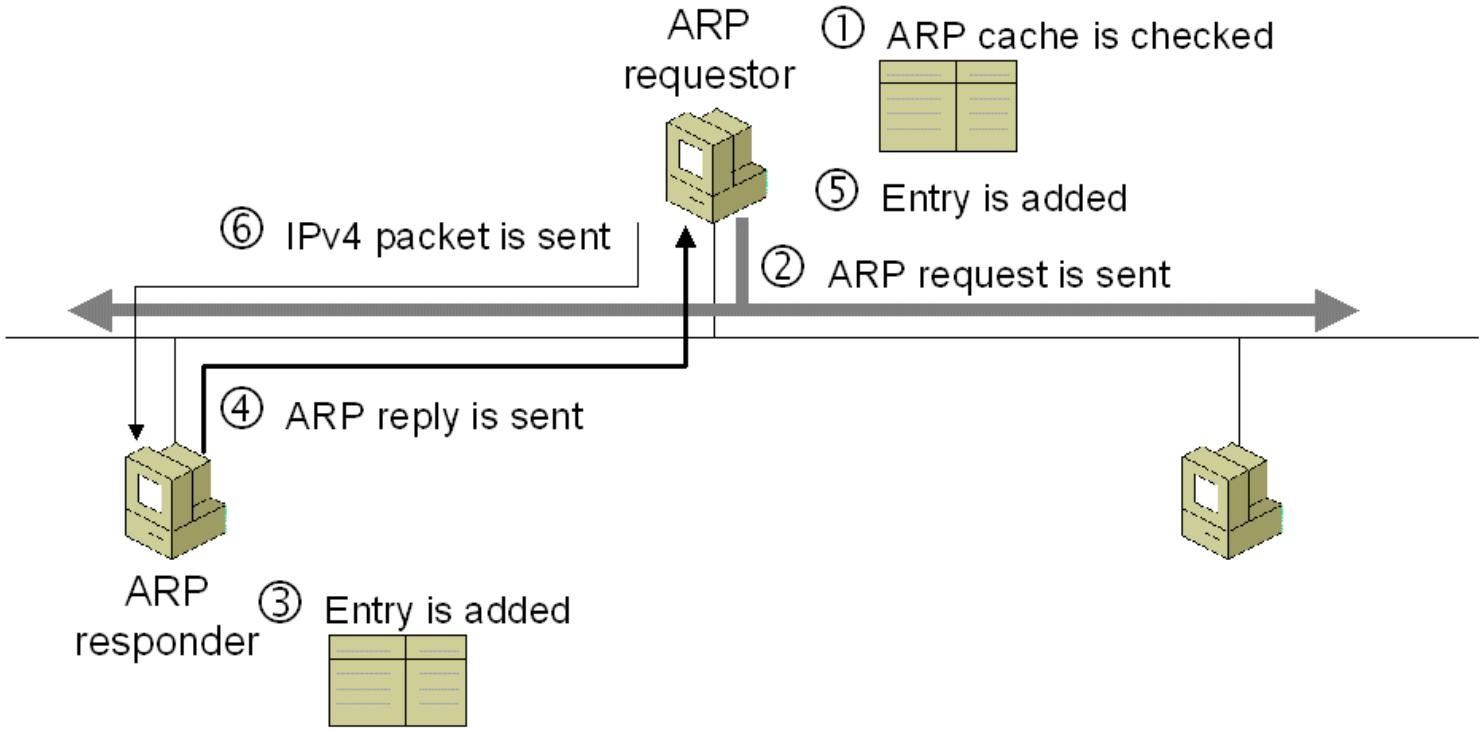
- Used for monitoring, or for Intrusion Detection Systems (IDS)
- Overcomes segmentation
- One port configured to receive copies of all packets from all other ports
- Only feasible on managed, enterprise level switches

ARP Cache Poisoning

- Address Resolution Protocol
- Cache poisoning
  - Allows you to intercept communications between two or more network devices (that you wouldn't normally see their traffic)

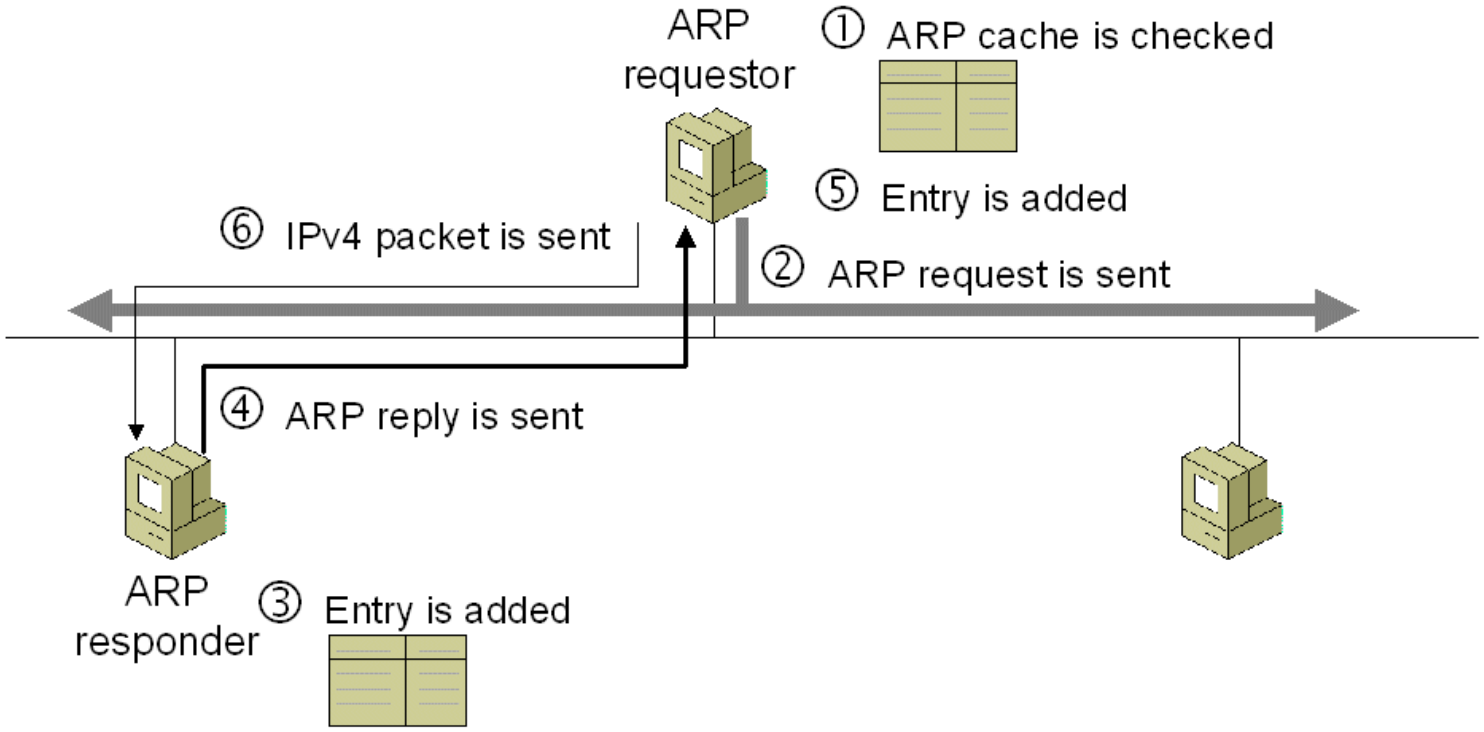
ARP Process

- Address Resolution Protocol resolves known IP addresses to unknown MAC addresses
- Resolves known IP addresses to unknown physical addresses

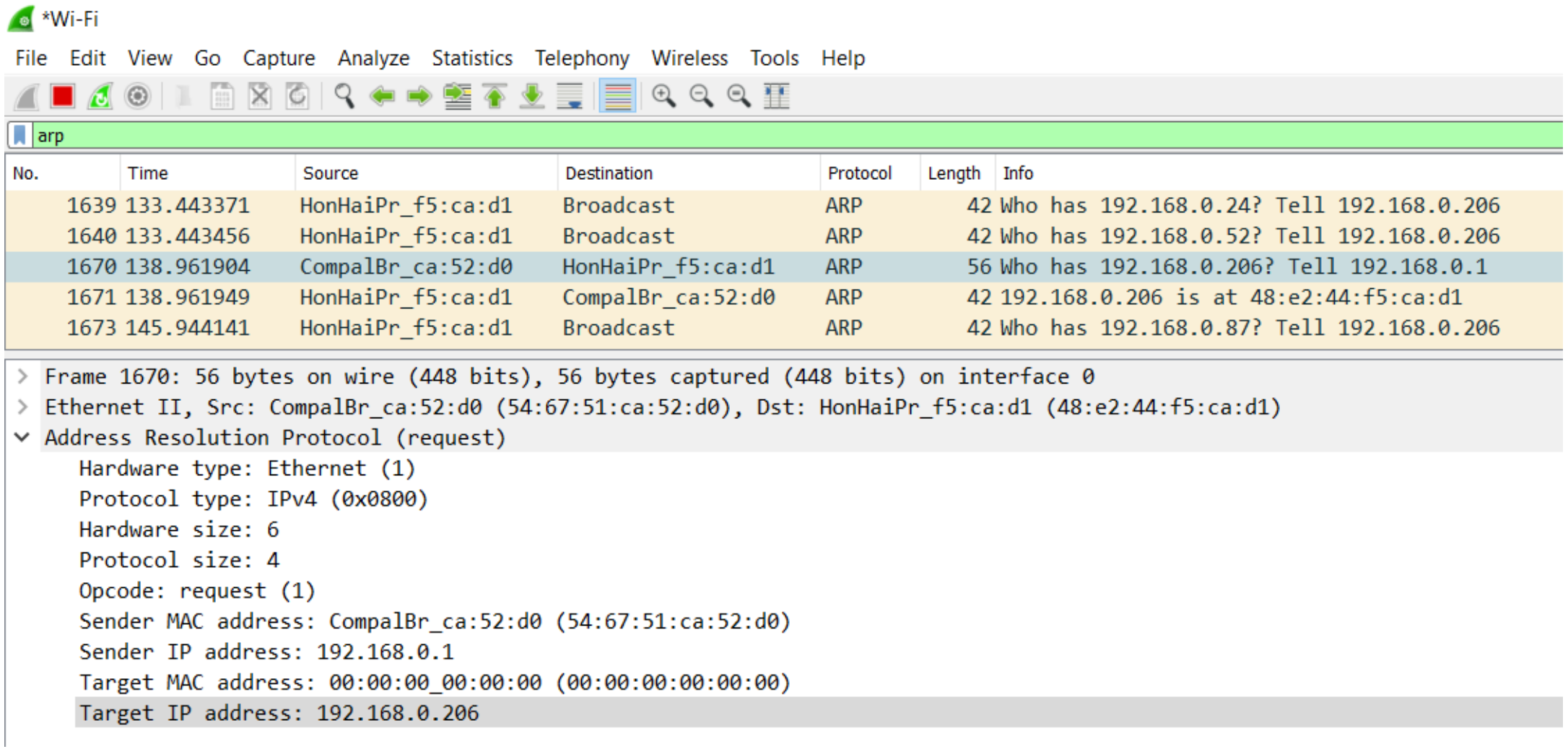


ARP Process

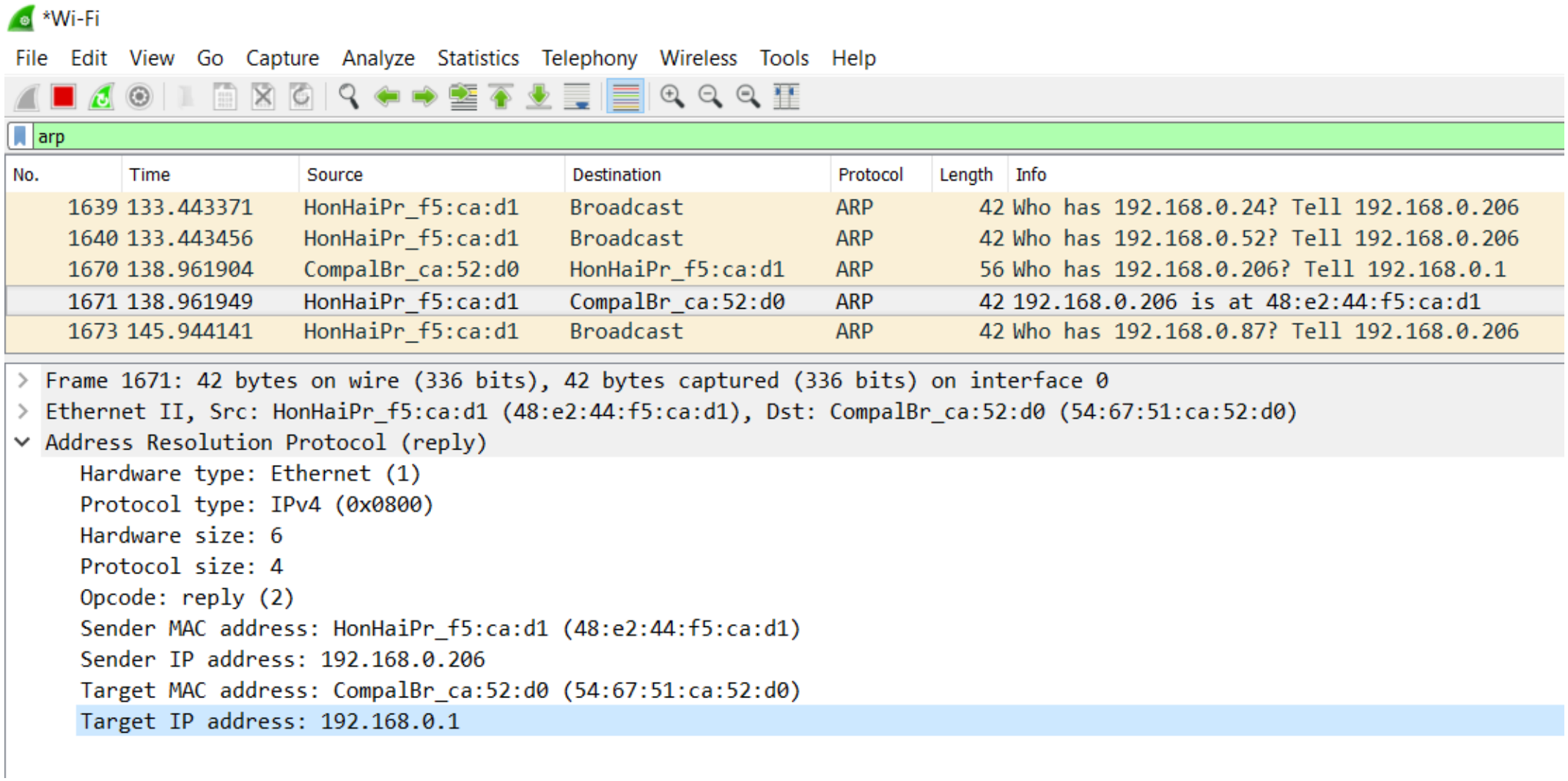
- Address Resolution Protocol resolves known IP addresses to unknown MAC addresses
- Resolves known IP addresses to unknown physical addresses



ARP


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
1639 133.443371 HonHaiPr_f5:ca:d1 Broadcast ARP 42 Who has 192.168.0.24? Tell 192.168.0.206
1640 133.443456 HonHaiPr_f5:ca:d1 Broadcast ARP 42 Who has 192.168.0.52? Tell 192.168.0.206
1670 138.961904 CompalBr_ca:52:d0 HonHaiPr_f5:ca:d1 ARP 56 Who has 192.168.0.206? Tell 192.168.0.1
1671 138.961949 HonHaiPr_f5:ca:d1 CompalBr_ca:52:d0 ARP 42 192.168.0.206 is at 48:e2:44:f5:ca:d1
1673 145.944141 HonHaiPr_f5:ca:d1 Broadcast ARP 42 Who has 192.168.0.87? Tell 192.168.0.206
Frame 1670: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Ethernet II, Src: CompalBr_ca:52:d0 (54:67:51:ca:52:d0), Dst: HonHaiPr_f5:ca:d1 (48:e2:44:f5:ca:d1)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: CompalBr_ca:52:d0 (54:67:51:ca:52:d0)
Sender IP address: 192.168.0.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.0.206

ARP


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
1639 133.443371 HonHaiPr_f5:ca:d1 Broadcast ARP 42 Who has 192.168.0.24? Tell 192.168.0.206
1640 133.443456 HonHaiPr_f5:ca:d1 Broadcast ARP 42 Who has 192.168.0.52? Tell 192.168.0.206
1670 138.961904 CompalBr_ca:52:d0 HonHaiPr_f5:ca:d1 ARP 56 Who has 192.168.0.206? Tell 192.168.0.1
1671 138.961949 HonHaiPr_f5:ca:d1 CompalBr_ca:52:d0 ARP 42 192.168.0.206 is at 48:e2:44:f5:ca:d1
1673 145.944141 HonHaiPr_f5:ca:d1 Broadcast ARP 42 Who has 192.168.0.87? Tell 192.168.0.206
Frame 1671: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HonHaiPr_f5:ca:d1 (48:e2:44:f5:ca:d1), Dst: CompalBr_ca:52:d0 (54:67:51:ca:52:d0)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HonHaiPr_f5:ca:d1 (48:e2:44:f5:ca:d1)
Sender IP address: 192.168.0.206
Target MAC address: CompalBr_ca:52:d0 (54:67:51:ca:52:d0)
Target IP address: 192.168.0.1

ARP

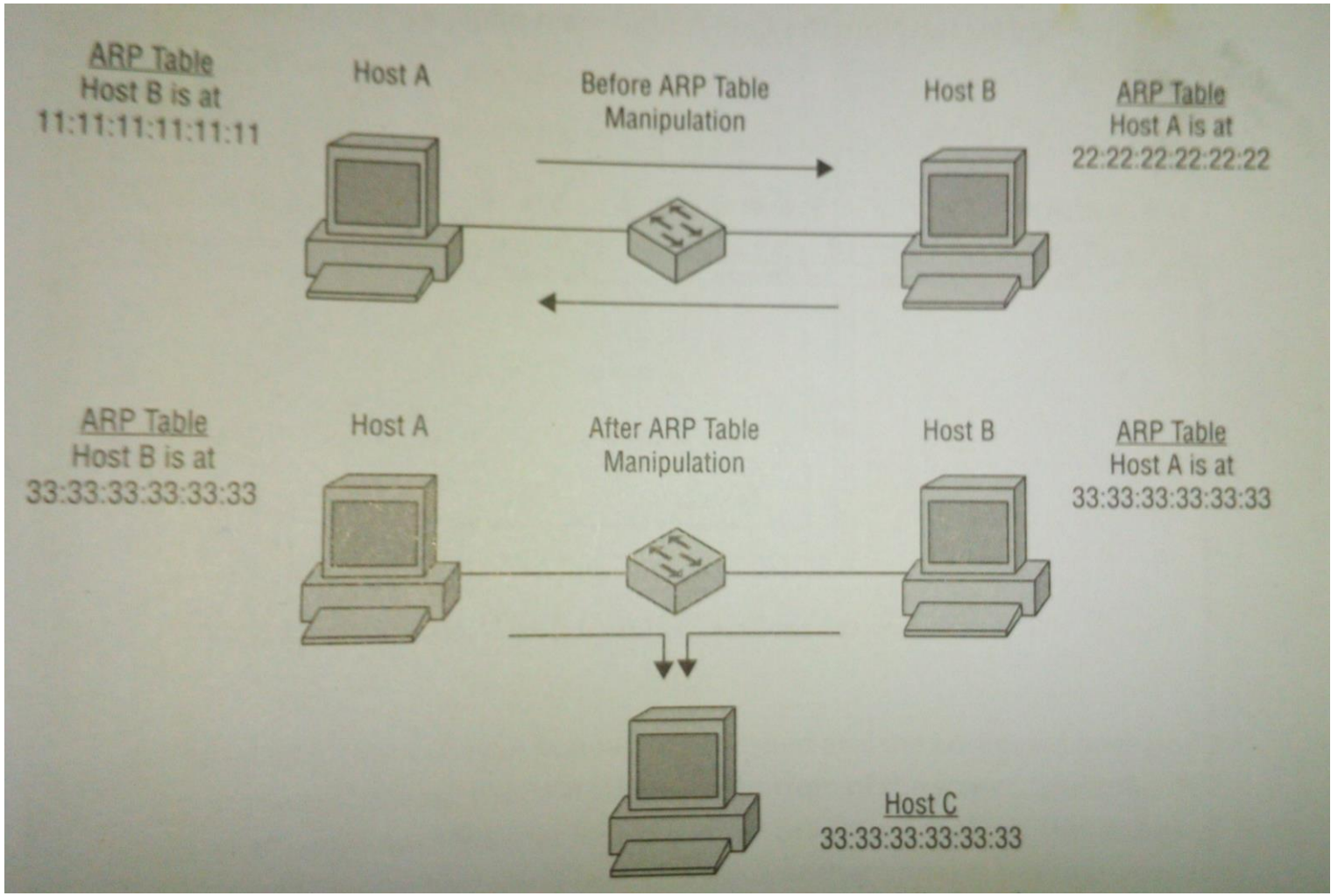
- ARP cache stores the IP address, MAC Address and a timer
  - 2 minutes on Windows, 15 on Linux
- View ARP Cache using **C:\arp –a**

```
Interface: 192.168.0.206 --- 0x12
  Internet Address      Physical Address      Type
  192.168.0.1           54-67-51-ca-52-d0     dynamic
  192.168.0.157         60-e3-27-d8-4d-c7     dynamic
  192.168.0.207         bc-03-08-a5-9f-95     dynamic
  192.168.0.248         38-06-0a-00-28-27     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
```

ARP Cache Poisoning

- ARP cache poisoning works by sending unsolicited ARP **replies**
- System trusts that replies come from the correct device
- ARP has no mechanism to verify corresponding device is who it says it is
- Some systems accept ARP replies even when no request has been made
- Also know as ***ARP Spoofing,*** involves sending spoofed arp replies to the switch and other devices to steer traffic to the sniffer
- Devices place this information into their ARP Cache and map attacker to the spoofed device.
- MAC Address being spoofed is usually the switch, so all traffic can be captured.
- Facilitates Man-in-the-Middle Attacks

ARP Cache Poisoning



ARP Cache Poisoning

- Attacker can now capture all network traffic
- Intercept and inspect traffic
- Many types of exploits including modification, replay, spoofing, impersonation attacks
- Tools for this type of attack include Cain & Abel, Ettercap
- Defence Tools include xARP, ARPwatch, IDS systems

Flooding

- MAC Flooding is another technique used to redirect traffic so it can be captured
- Brute-force attack
- Attempts to overload CAM tables in a switch
- In older switches amount of memory is limited
- If CAM table fills, and can't hold more entry, some switches revert to a *failover* state
  - This means all frames are broadcast out all ports (like a hub)
  - Attacker can now capture/sniff traffic
- Flooding injects large amount of data into the network, which can draw attention
- May disable a port
- Sniffer should be located on a second system, not on the same as the flooding system

DHCP Redirection

- DHCP can be targeted by means of a rogue DHCP server
  - Attacker needs to set up their own DHCP server
  - Broadcasts forged DHCP requests in attempt to lease all of the available DHCP addresses in the DHCP scope (resource starvation)
  - Legitimate users now unable to obtain or renew IP addresses from the server
  - Attacker now starts their rogue server and sends out DHCP IP addresses with their address as the new gateway
  - End users now access the Internet, or other networks, via the attackers IP, which allows the attacker to sniff/capture all network traffic.
  - Tools include Gobbler, Yersinia, DHCPstarve

ICMP Redirect

- Misuse of ICMP redirect (Type 5)
- A redirect is normally sent by the router to a host to indicate a better route exists to a destination
- A host will accept an ICMP redirect as long as it appears valid and appears to come from the default gateway for the destination its redirecting
- Once redirected, traffic is passed to attackers system
- Tools include:
- Ettercap https://github.com/ettercap/ettercap
- Interceptor-NG http://sniff.su/download.html
- Netwox: http:sourceforge.net/projects/ntwox/files/netwib%20netwox%20and%20netwag

Preventing Packet Capture

- Several ways to enforce port security and block unauthorised redirecting
- These techniques include:
- Dynamic address inspection (DAI)
- DHCP snooping

Dynamic Address Inspection

- Two redirection techniques mentioned previously include ARP cache poisoning and flooding
- Dynamic Address Resolution Protocol Inspection (DAI) can stop these attacks
- DAI is a security feature that validates ARP packets
- DAI functions by performing IP-to-MAC binding inspection. Results stored in a trusted lookup table
  - DAI intercepts all ARP requests/responses, verifies that each is valid, silently drops invalid packets.
  - DAI can be used to define trusted and untrusted interfaces.
  - DAI sets threshold for incoming ARP traffic. If rate exceeds threshold, then port is disabled.

DHCP Snooping

- DHCP snooping, implemented at data-link layer on switches can stop attacks and block unauthorised DHCP servers.
- Layer 2 switch can inspect frames received on a specific port to check if they are legitimate.
- Source and destination MAC addreses are defined, and packets that don't match are dropped.
- Can log messages/alerts
- Cisco devices

Detecting Packet Capture

Several techniques for packet capture detection

- Monitoring ARP traffic
- Watching DNS transactions
- Listening for responses to invalid packets
- Testing for network latency
- Performing local detection

Monitoring ARP traffic

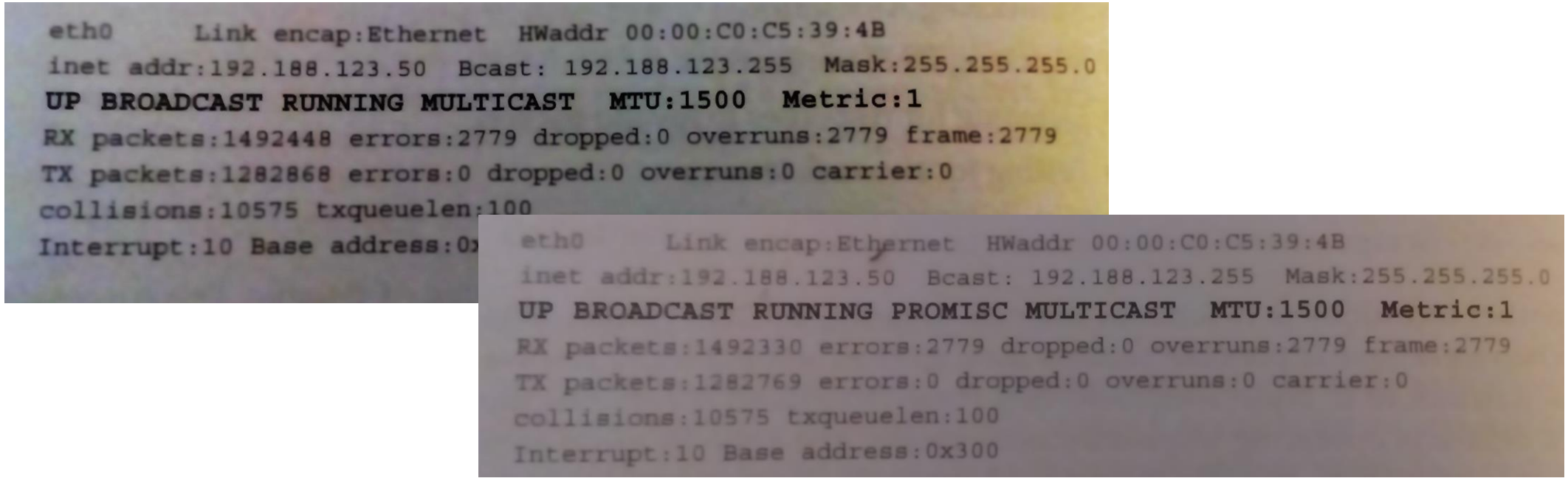
- When a device is in promiscuous mode, it accepts all packets sent to it.
- The idea is to see which devices respond to ARP requests sent with an invalid MAC address
- If they respond, then it is suspicious, and worth further investigation
- Nmap script to test it:
- Nmap –sV –script=sniffer-detect <target IP address>

Watching DNS Traffic

- Look for unusual amounts of DNS traffic
- Most sniffers automatically resolve domain names to IP addresses
- Detecting those DNS queries may indicate a device is operating in promiscuous mode
- Invalid packets can also be used to test for devices in promiscuous mode
- Example: a fake Ethernet frame with an invalid address can be sent with a valid packet containing a ping (ICMP) request.
- If device is in promiscuous mode it may respond to the packet
- If not, it should drop the packet

Network Latency

- This technique works by tracking the request-and-response times of ping packets
  - Times vary slightly depending on whether device is in promiscuous mode
- To check if a device is in promiscuous mode: ***ifconfig***

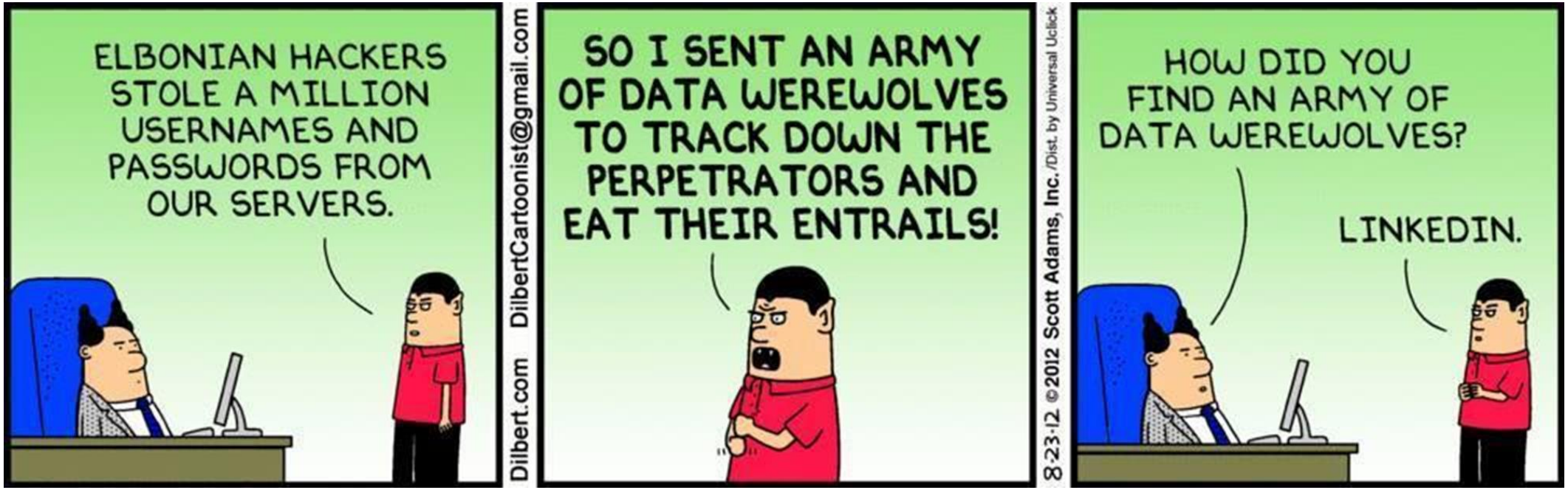


Network Latency

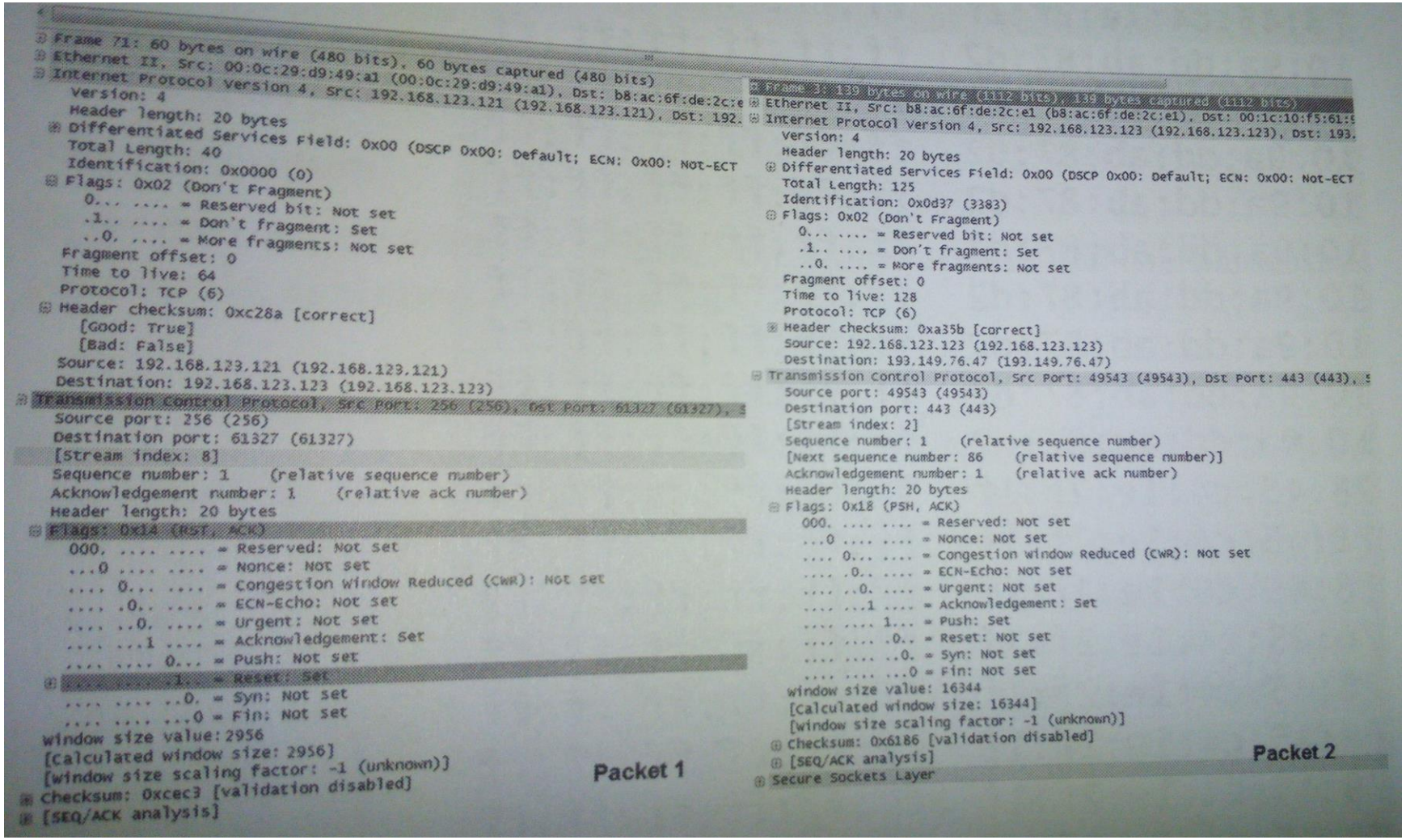
- IDS can be used to detect promiscuous devices
- Replacement *ifconfig*, which doesn't report promiscuous mode
- One-way data cable, means a device can receive traffic but not transmit.

Honeytokens

- A type of honeypot to lure in an attacker, or anyone sniffing a network
- Example: a cleartext FTP password could be used to log into a (fake) FTP service on the network.
- Any non-planned access to this service is clearly not legitimate, and would indicate someone is monitoring traffic.
- You could configure an IDS, such as Snort, to alert you to any network traffic using that honeytoken.
- Downside is that honeytokens don't tell you where the promiscuous device is.
- Also, might not indicate there is promiscuous device (honeytoken could have been obtained by other means)


ELBONIAN HACKERS STOLE A MILLION USERNAMES AND PASSWORDS FROM OUR SERVERS.
Dilbert.com DilbertCartoonist@gmail.com
SO I SENT AN ARMY OF DATA WEREWOLVES TO TRACK DOWN THE PERPETRATORS AND EAT THEIR ENTRAILS!
8-23-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
HOW DID YOU FIND AN ARMY OF DATA WEREWOLVES?
LINKEDIN.

Lab exercises



Lab exercises

- 1. Look at packets 1 and 2. Which OS is each?
- Moodle Wireshark challenge