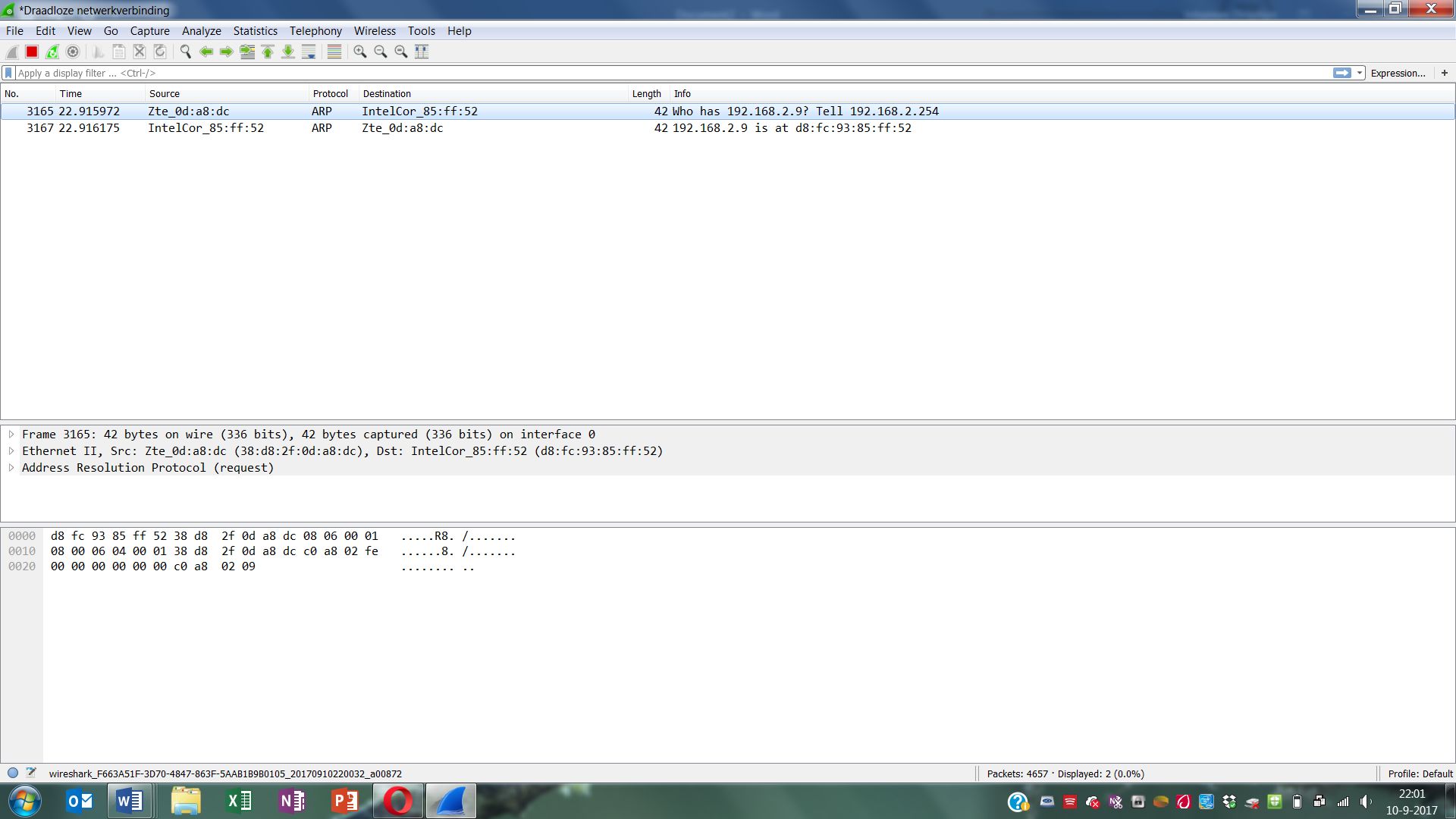
Zoals weet, wordt ARP gebruikt om MAC adressen naar IP adressen op een intern netwerk in kaart te brengen. De router en de switches sturen ARP-verzoeken (broadcasts) uit naar alle MAC-adressen op het netwerk, waarin ze worden gevraagd om te reageren met hun IP-adressen. Elk systeem zal reageren met hun IP-adres en de switch of ander apparaat zal dan een kleine database (ARP-cache) aanmaken waar de MACs met de bijbehorende IP adressen in staan, een wie-is-wie op het lokale netwerk

ARP betekent Address Resolutie Protocol. Een bekende tool binnen KALI Linux is Netdiscover. Deze tool maakt gebruikt van het ARP protocol om een mogelijk doelwit in kaart te brengen.

Voordat we verder gaan met netdiscovery gaan we eerst het normale ARP verkeer bekijken op het netwerk.

PUNT 1

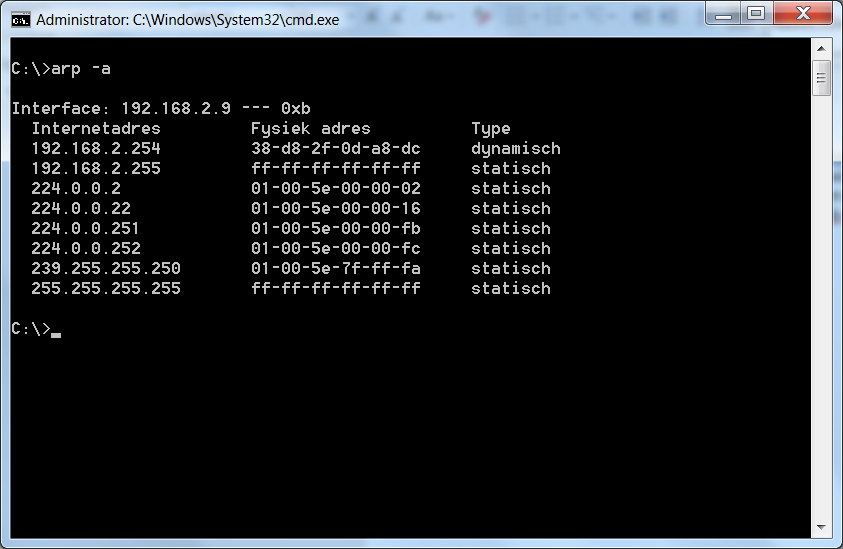
Open Wireshark en capture het netwerkverkeer op je verbinding. Stop na een halve minuut de capture. Typ in de filter ARP en bekijk of je ARP-pakketten kunt vinden. Zie het voorbeeld hieronder.



De computer stuurt met ieder pakket het MAC adres mee van het ontvangende apparaat. Als de computer die niet weet stuurt het een ARP request, een broadcast naar alle computers in het netwerk (dat is het WHO HAS pakket hierboven). De computer die het desbetreffende IP heeft, geeft antwoord door het eigen MAC adres te versturen. (Dat zie je in je Wireshark als het “tweede” ARP pakket met IS AT in de regel.

Je kunt de database (de ARP cache op je computer bekijken via je CMD-prompt met:

ARP -a



VUL DE TABELLEN IN MET JE EIGEN GEGEVENS UIT JOUW WIRESHARK SESSIE

|  |  |
| --- | --- |
| Address Resolution Protocol | REQUEST |
| Hardware type: |  |
| Protocol type: |  |
| Hardware size: |  |
| Protocol size: |  |
| Opcode: |  |
| Sender MAC address: |  |
| Sender IP address: |  |
| Target MAC address: |  |
| Target IP address: |  |

|  |  |
| --- | --- |
| Address Resolution Protocol | REPLY |
| Hardware type: |  |
| Protocol type: |  |
| Hardware size: |  |
| Protocol size: |  |
| Opcode: |  |
| Sender MAC address: |  |
| Sender IP address: |  |
| Target MAC address: |  |
| Target IP address: |  |

In beide pakketten is de lengte van het “hardware size” veld 6. Kan je dat verklaren?

Een MAC adres is 48 bits = 6 bytes

In beide pakketten is de lengte van het “IP size” veld 4. Kan je dat verklaren?

En IP pakket is 32 bits = 4 bytes

Wat is de OPcode (operations-code) in de beide velden? Kan je dat verklaren?

OPcode 1 = Request; Opcode 2 is Reply.

Waarom betekent het als er bij een MAC adres alleen maar nullen staan?

Dat is een broadcast (alle computers)

Staan in de reply ook een MAC adres op 0?

Nee, het is geen broadcast maat een unicast

Netdiscover

Netdiscover is een simpele tool die op een netwrksegment syste

Geef het ommando

netdiscover -help

Usage: netdiscover [-i device] [-r range | -p] [-s time] [-n node] [-c count] [-f] [-S]

Van de bovenstaande

-i device: your network device

-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8

-p passive mode do not send anything, only sniff

If -p or -r aren't enabled, netdiscover will scan for common lan addresses