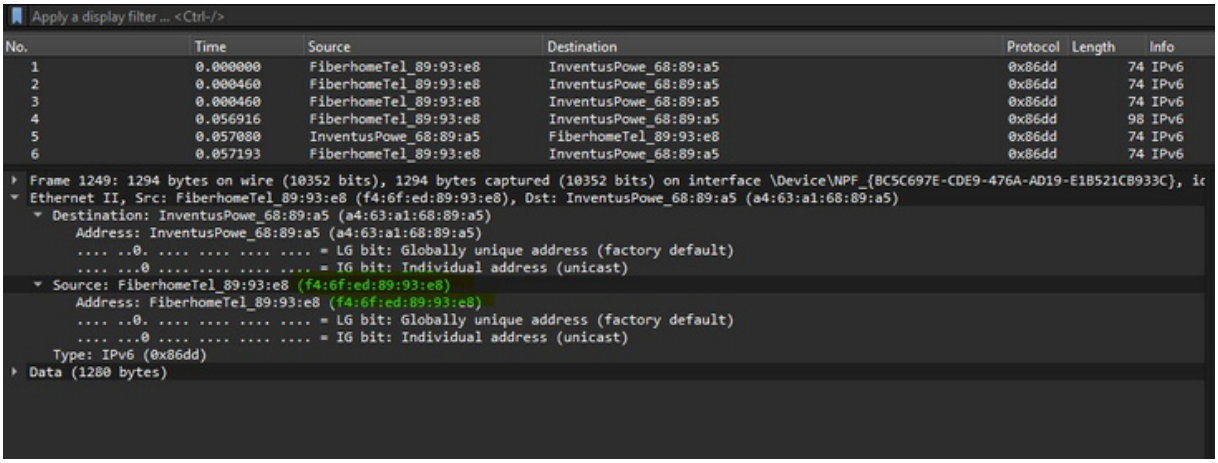
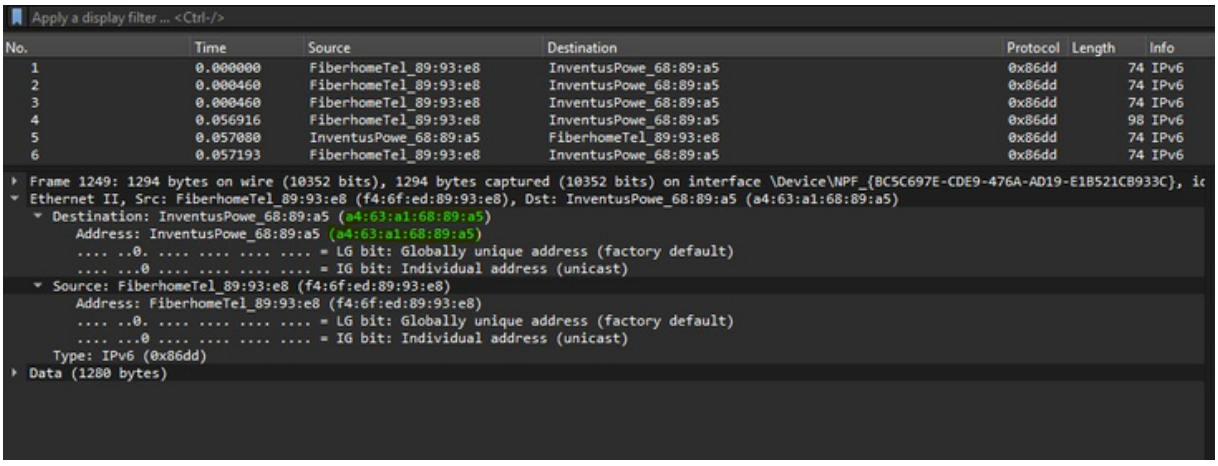
Laboratório Ethernet Wireshark
Alunos: Eduardo Henrique

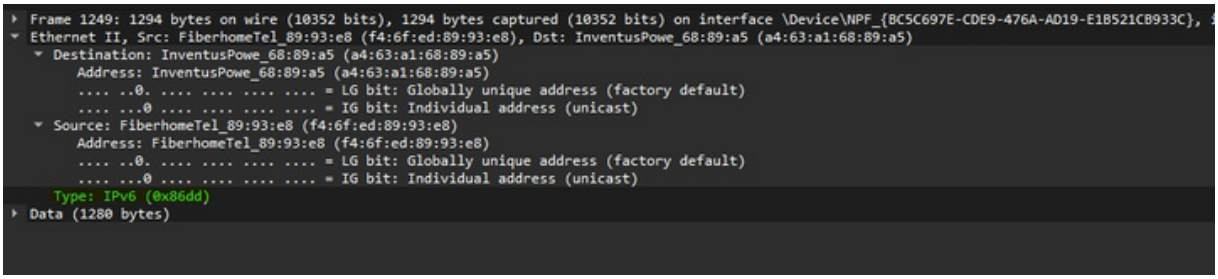
1. Qual é o endereço Ethernet de 48 bits do seu computador?



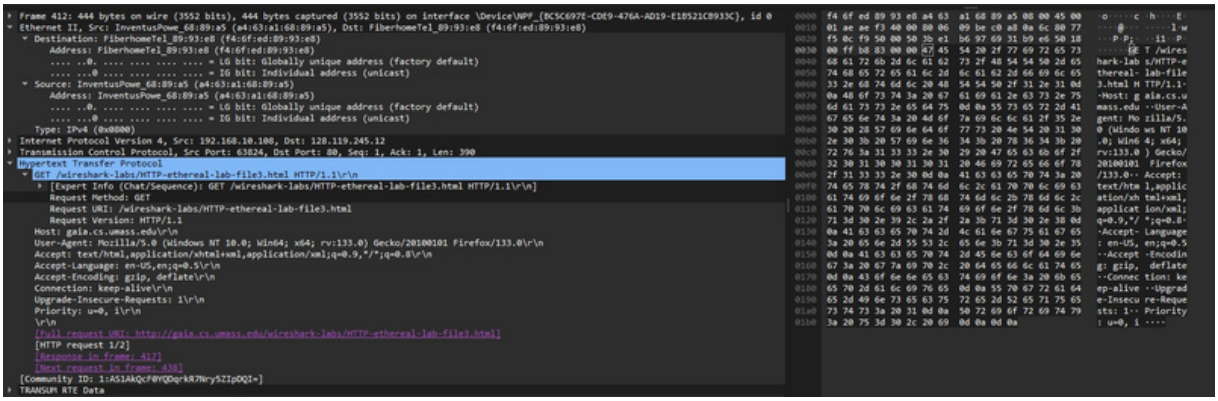
2. Qualéoendereçodedestinode48bitsnoquadroEthernet?EsteéoEthernet endereço de gaia.cs.umass.edu? (Dica: a resposta é não). Qual dispositivo tem isso como endereço Ethernet? [Nota: esta é uma pergunta importante, e uma que os alunos às vezes erram.



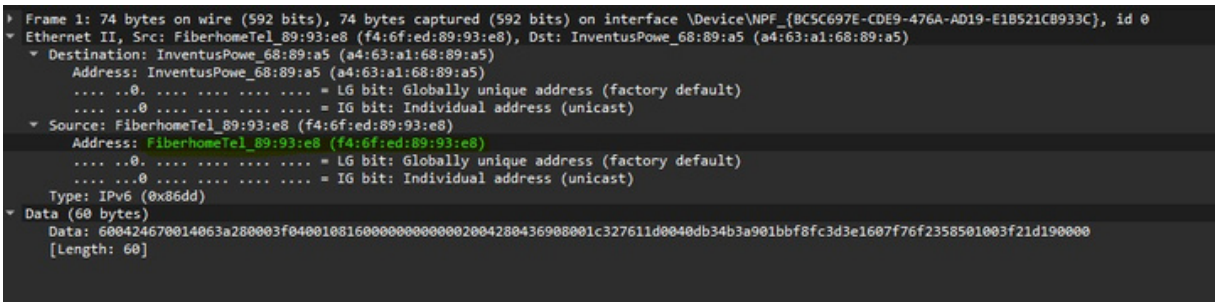
3. Dêovalorhexadecimalparaocampo Frametypededoisbytes.Aqual protocolo de camada superior isso corresponde?



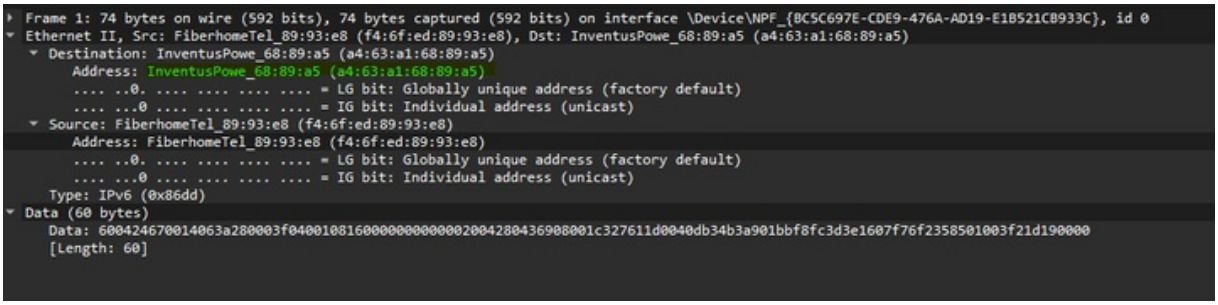
4. QuantosbytesdesdeoiníciodoquadroEthernetoASCII “G” em “GET” aparece no quadro Ethernet?



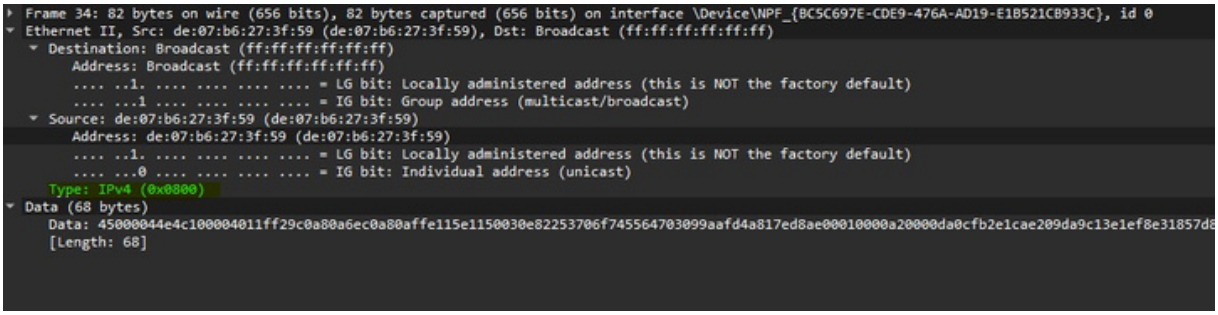
5. Qualéovalordoendereçodeorigem Ethernet? Esteéoendereçodoseu computador, ou de gaia.cs.umass.edu (Dica: a resposta é não). Qual dispositivo tem isso como endereço Ethernet?



6. Qualéoendereçodedestinonoquadro Ethernet? EsteéoendereçoEthernet do seu computador?



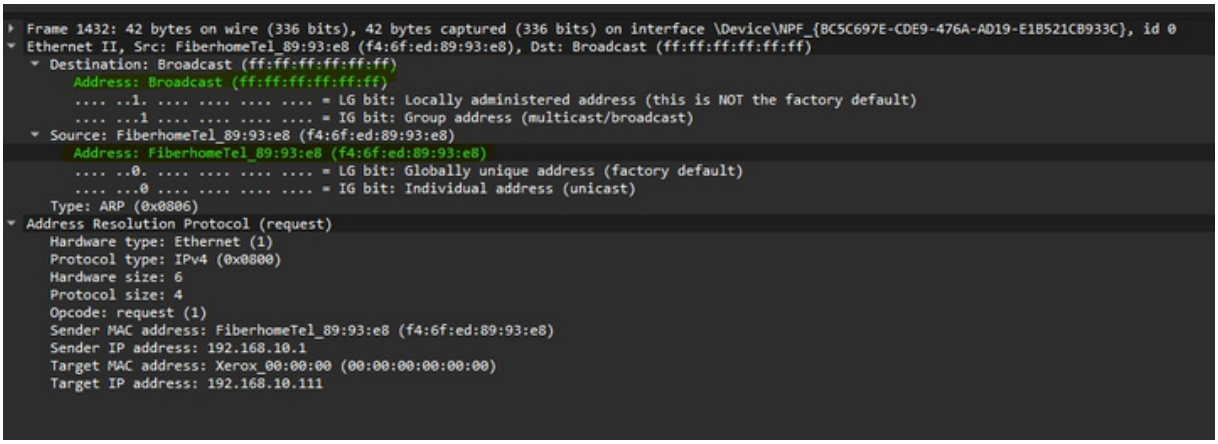
7. DêovalorhexadecimalparaocampoFrametypededoisbytes.Aqual protocolo de camada superior isso corresponde?



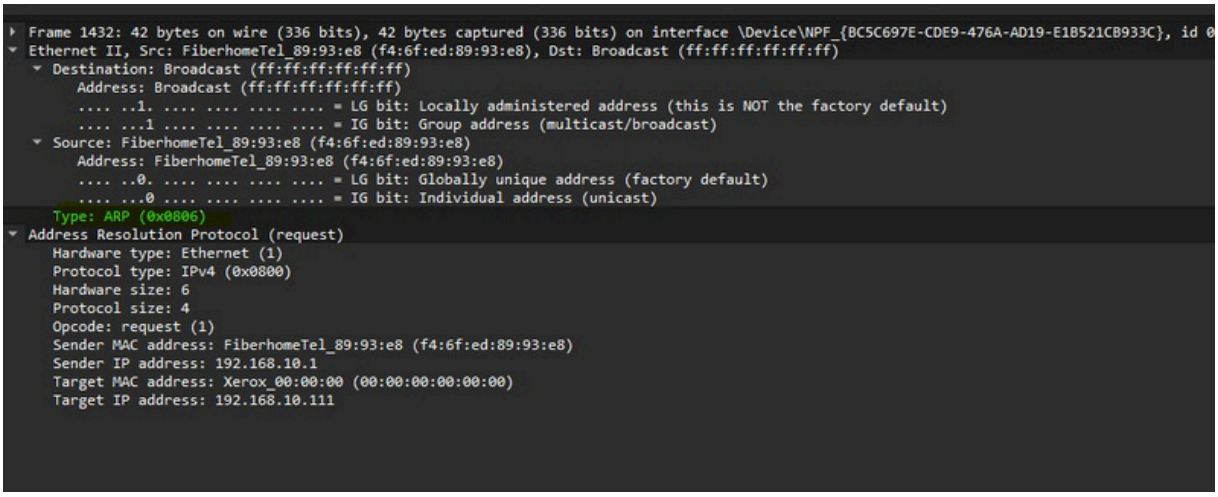
8. QuantosbytesdesdeoiníciodoquadroEthernetoASCII“O”em“OK”(ouseja, o código de resposta HTTP) aparece no quadro Ethernet?

9. AnoteoconteúdodocacheARPdoseucomputador.Qualéosignificadode cada valor de coluna?

10. Quaissãoosvaloreshexadecimaisparaosendereçosdeorigemedestinono Quadro Ethernet contendo a mensagem de solicitação ARP?



11. Dêovalorhexadecimalparaocampodotipodequadro Ethernetdedois bytes. O que isso corresponde ao protocolo da camada superior?



12. BaixeaespecificaçãoARPde ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. Uma discussão legível e detalhada sobre ARP também está em http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

a) Quantos bytes desde o início do quadro Ethernet o Início do campo opcode ARP?

Resposta: 6 bytes.

b) Qual é o valor do campo opcode dentro da parte ARP-payload do Quadro Ethernet no qual uma solicitação ARP é feita?

Resposta: 0x0001

c) A mensagem ARP contém o endereço IP do remetente?

Resposta: Sim. O campo Sender Protocol Address no cabeçalho ARP contém o endereço IP do remetente.

d) Onde na solicitação ARP a “pergunta” aparece – a Ethernet endereço da máquina cujo endereço IP correspondente está sendo consultado?

Resposta: No campo Target Hardware Address.

13. AgoraencontrearespostaARPquefoienviadaemrespostaàsolicitação ARP.

a) Quantos bytes desde o início do quadro Ethernet o Início do campo opcode ARP?

Resposta: 20º byte.

b) Qual é o valor do campo opcode dentro da parte ARP-payload do Quadro Ethernet no qual uma resposta ARP é feita?

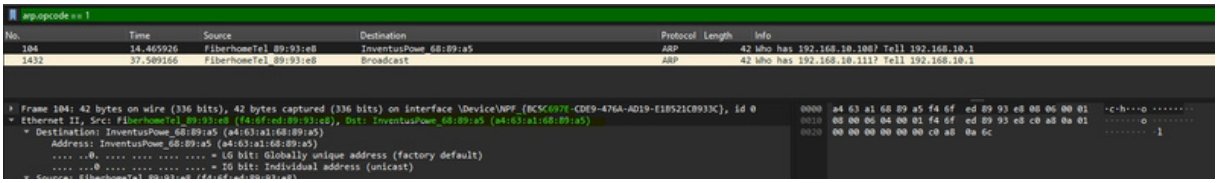
Resposta: 0x0002

c) Onde na mensagem ARP aparece a “resposta” à solicitação ARP anterior – o endereço IP da máquina que tem o endereço Ethernet cujo endereço IP correspondente está sendo consultado?

Sender Hardware Address: Contém o endereço Ethernet do dispositivo que respondeu.

Sender Protocol Address: Contém o endereço IP associado ao endereço Ethernet do remetente.

14. Quaissãoosvaloreshexadecimaisparaosendereçosdeorigemedestinono quadro Ethernet que contém a mensagem de resposta ARP?



15. Abra o arquivo de rastreamento ethernet-ethereal-trace-1 em http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. O primeiro e o segundo pacotes ARP neste rastreamento correspondem a uma solicitação ARP enviada pelo computador que executa o Wireshark, e a resposta ARP enviada ao computador que executa o Wireshark pelo computador com o endereço Ethernet solicitado pelo ARP. Mas há ainda outro computador nesta rede, conforme indicado pelo pacote 6 – outra solicitação ARP. Por que não há resposta ARP (enviada em resposta à solicitação ARP no pacote 6) no rastreamento do pacote?

Resposta: O mais provável é que o endereço IP alvo no pacote 6 não corresponda a nenhum dispositivo ativo na rede.