Neste laboratório, capturaremos um rastreamento de uma interface WiFi 802.11 sem fio em nosso computador/laptop. Aqui estão as ações tomadas, supondo que você já esteja conectado a uma rede Wi-Fi (que chamaremos de sua rede doméstica), quando a coleta de rastreamento for iniciada:

- Faça uma solicitação HTTP para http://gaia.cs.umass.edu/wireshark-labs/alice.txt (basta clicar no link)
- Faça um pedido para http://www.cs.umass.edu (basta clicar no link)
- Desconecte-se da sua rede doméstica
- (etapa opcional) Tente se conectar a outra rede sem fio 802.11 cujos anúncios de beacon estão sendo recebidos e para a qual você não tem acesso e, portanto, sua tentativa de conexão falhará.
- Conecte-se novamente (com sucesso) à sua rede doméstica.

Para responder a algumas das perguntas abaixo, você deve examinar os detalhes no campo nformações (Info) na coluna mais à direita da tela do Wireshark; para responder a outras perguntas, você precisará se aprofundar no quadro "Protocolo 802.11" e nos subcampos na janela do meio do Wireshark.

1. Quais são os SSIDs dos dois pontos de acesso que estão emitindo a maioria dos quadros de beacon neste rastreamento? [Dica: olhe para o Campo de informações. Para exibir apenas quadros de sinalização, insira wlan.fc.type_subtype == 8 no filtro de exibição do Wireshark].
   R: "30 Munroe St" e "linksys12"
2. Qual canal 802.11 está sendo usado por ambos os pontos de acesso [Dica: você precisará se aprofundar nas informações de rádio em um quadro de beacon 802.11]
   R: Canal 6 (2,437GHz)

Agora vamos dar uma olhada no quadro de beacon enviado em t=0,085474.

3. Qual é o intervalo de tempo entre as transmissões de quadros de beacon deste ponto de acesso (AP)? (Dica: esse intervalo de tempo está contido em um campo dentro do próprio quadro do beacon)."
   R: 0,102400s
4. Qual (em notação hexadecimal) é o endereço MAC de origem no quadro de beacon deste ponto de acesso? Lembre-se da Figura 7.13 no texto que a origem, o destino e o BSS são três endereços usados em um quadro 802.11. Para obter uma discussão detalhada sobre a

estrutura do quadro 802.11, consulte a seção 9.2.3 - 9.2.4.1 no documento de padrões IEEE 802.11, extraído aqui.
R: 00:16:b6:f7:1d:51

5. Qual (em notação hexadecimal) é o endereço MAC de destino no quadro do beacon de 30 Munroe St?
   R: ff:ff:ff:ff:ff:ff
6. Qual (em notação hexadecimal) é o MAC BSS ID no quadro do beacon de 30 Munroe St?
   R: 00:16:b6:f7:1d:51
7. Os quadros de beacon do ponto de acesso 30 Munroe St anunciam que o ponto de acesso pode suportar quatro taxas de dados e oito "taxas suportadas estendidas" adicionais. Quais são essas taxas? [Nota: os traços foram tirados em um AP bastante antigo].
   R: As quatro taxas são 1, 2, 5,5, e 11 (Mbit/s). As extendidas são: 6, 9, 12, 18, 24, 36, 48 e 54 (Mbit/s)
8. Encontre o quadro 802.11 que contém o segmento TCP SYN para esta primeira sessão TCP (que faz download alice.txt) em t=24.8110. Quais são os três campos de endereço MAC no quadro 802.11? Qual endereço MAC neste quadro corresponde ao host sem fio (forneça a representação hexadecimal do endereço MAC do host)? Para o ponto de acesso? Para o roteador do primeiro salto? Qual é o endereço IP do host sem fio que envia esse segmento TCP? Qual é o endereço IP de destino para o segmento TCP syn?
   R: 1 - Dest: 00:16:b6:f7:1d:51, 2 - Source: 00:13:02:d1:b6:4f, 3 - BSSID: 00:16:b6:f7:1d:51, o host sem fio é o transmitter, neste caso é o Source (00:13:02:d1:b6:4f), Ponto de acesso é o BSSID (00:16:b6:f7:1d:51), Roteador do primeiro salto é o Dest (00:16:b6:f7:1d:51), Endereço de IP do Host sem fio é o endereço de origem (192.168.1.109), o destino é o servidor (128.119.245.12)
9. O endereço IP de destino desse TCP SYN corresponde ao host, ponto de acesso, roteador de primeiro salto ou servidor web de destino?
   R: Servidor web de destino
10. Encontre o quadro 802.11 que contém o segmento SYNACK para esta sessão TCP recebida em t=24.8277 Quais são os três campos de endereço MAC no quadro 802.11? Qual endereço MAC neste quadro corresponde ao host? Para o ponto de acesso? Para o roteador do primeiro salto? O endereço MAC do remetente no quadro corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado nesse datagrama? (Dica: revise a Figura 6.19 no texto se não tiver certeza de como responder a esta pergunta ou à parte correspondente da pergunta anterior. É particularmente importante que você entenda isso).

R: 1 - Dest: 00:13:02:d1:b6:4f, 2 - Source: 00:16:b6:f7:1d:51, 3 - BSSID: 00:16:b6:f7:1d:51, o host sem fio é o receiver, neste caso é o Dest (00:13:02:d1:b6:4f), Ponto de acesso é o BSSID (00:16:b6:f7:1d:51), Roteador do primeiro salto é o Source (00:16:b6:f7:1d:51), O endereço MAC do remetente não é o mesmo do endereço MAC do dispositivo que enviou o segmento TCP, pois a rede de origem é diferente da rede de destino, logo, o MAC presente é do gateway da rede local

11. Quais são as duas ações tomadas (ou seja, os quadros são enviados) pelo host no rastreamento logo após t = 49, para encerrar a associação com o AP 30 Munroe St que estava inicialmente em vigor quando a coleta de rastreamento começou? (Dica: uma é uma ação de camada IP e a outra é uma ação de camada 802.11).
    R: A ação da camada de IP é um DHCP Release, onde o dispositivo libera o IP. A outra ação é o Deauthentication, onde a placa de rede do dispositivo final efetua um "logout" no ponto de acesso.
12. Vejamos primeiro os quadros AUTHENTICATION. Em t = 63,1680, nosso host tenta se associar ao AP 30 Munroe St . Use o filtro de exibição do Wireshark wlan.fc.subtype == 11 para mostrar os quadros de AUTHENICATION enviados do host para o AP e vice-versa. Que forma de autenticação o host está solicitando?
    R: Authentication Algorithm: Open System (0). Uma autenticação sem senha.
13. Qual é o valor SEQ de autenticação (número de sequência de autenticação) desse quadro de autenticação do host para o AP?
    R: Authentication SEQ: 0x0001
14. A resposta do AP à solicitação de autenticação é recebida em t = 63,1690. O AP aceitou a forma de autenticação solicitada pelo host?
    R: Status code: Successful (0x0000). Sim, a autenticação foi efetuada com sucesso.
15. Qual é o valor SEQ de autenticação desse quadro de autenticação do AP para o host?
    R: Authentication SEQ: 0x0002
16. Quais taxas são indicadas no quadro como TAXAS SUPORTADAS. Não inclua em suas respostas quaisquer taxas que sejam indicadas como TAXAS DE SUPORTE ESTENDIDAS.
    R: Analisando o frame t = 63,1921, o ap suporta as seguintes faixas:
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
17. A RESPOSTA DE ASSOCIAÇÃO indica uma resposta de associação bem-sucedida ou malsucedida?
    R: Status code: Successful (0x0000), Indica sucesso
18. A taxa de suporte estendida mais rápida (maior) que o host ofereceu corresponde à taxa de suporte estendida mais rápida (maior) que o AP é capaz de fornecer?

R: Frame t = 63,1699 declara que suporta as seguintes taxas:
Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
Framet = t = 63,1921 declara que suporta as seguintes taxas:
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Logo, a maior taxa oferecida pelo host pode ser atendida pelo AP.