BCIT

COMP 3721 **作业 3**

**~~注意:~~**

- 提交一个 PDF 文件。
- 请根据教科书、讲义和课堂讨论作答，不要使用 ChatGPT 或 Google。

**Q1:**

对于目标 IP 地址 14.12.72.8/24，求出以下各项。
(a) 目标 IP 地址的二进制表示
(b) 子网掩码的二进制表示
(c) 子网掩码的点分十进制表示
(d) 该网段的第一个地址（即网络地址）
(e) 该网段的最后一个地址（即广播地址）
(f) 网络块的第一个主机地址
(g) 网络块的最后一个主机地址
(h) 网络块中的地址数量
(i) 网络块中最大主机数

**Q2:**

对于目标 IP 地址 200.107.16.17/18，找出以下内容。
(a) 目标 IP 地址（二进制）
(b) 子网掩码（二进制）
(c) 子网掩码（点分十进制）
(d) 区块的第一个地址（即网络地址）
(e) 区块的最后一个地址（即广播地址）
(f) 区块的第一个主机地址
(g) 区块的最后一个主机地址
(h) 区块中的地址数量
（i）块中主机的最大数量

**Q3:**

下载并安装 Wireshark（https://www.wireshark.org/）。打开 “trace.cap”（随作业提供）

g$_{nment}$ ) by either

- 双击抓包文件（如果该扩展名已关联到 Wireshark），或者
- 打开 Wireshark，点击 文件 → 打开 → 浏览并选择该文件。

通过应用正确的过滤器，截取显示以下内容的 Wireshark 屏幕。

- 每个问题一份抓包。
- 必须显示显示过滤器。
- 只需显示结果的前几行（如有）。

(a) 显示所有源地址为 192.168.100.102 的数据包。
(b) 显示所有源地址为 192.168.100.102 且目的地址为 142.104.193.247 的数据包。

(c) 显示所有 HTTP 数据包。
(d) 显示所有源地址为 192.168.100.102 的 TCP 数据包。
（e）显示所有 ICMP 数据包。

**App附录 – 一些 Wireshark 显示过滤器：**

- 比较规则
  - 英语：`eq`、`le`、`ge`、`lt`、`gt`、`ne`
  - 类 C：`==`、`<=`、`>=`、`<`、`>`、`!`
- 逻辑运算符
  - English: `and`, `or`, `xor`, `not`
  - C-like: `&&`, `||`, `^^`, `!`
- Boolean——当字段存在时，其值为 true。
  - 例如，`tcp.flags.syn` 在所有包含该标志的 TCP 数据包中均为存在，不论 SYN 标志是 0 还是 1。若只匹配设置了 SYN 标志的 TCP 数据包，则需要使用 `tcp.flags.syn == 1` 或 `tcp.flags.syn == True`。
- Addresses
  - o IPv4 地址：例如，`ip.addr == 192.168.0.1` o IPv4 源地址：例如，显示来自 192.168.100.102 的数据包 →
    ip.src == 192.168.100.102
  - 以太网（链路层/MAC）地址。例如，`eth.dst == ff:ff:ff:ff:ff:ff`

欲了解更多信息，请查阅 Wireshark 关于显示过滤表达式的文档（https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html）。

**— 作业 3 结束 —**