## **Activity File: Interpreting Protocols**

In this exercise, you'll continue to play the role of a security analyst at Acme Corp.

* Several raw network log captures were pulled from a potentially rogue employee, Sally Stealer.
* Your manager has tasked you with converting the raw binary data into a readable format and determining the protocol being used.
* Log file:

<https://uci.bootcampcontent.com/UCI-Coding-Bootcamp/uci-irv-virt-cyber-09-2021-u-c/-/blob/master/Lessons/08-Networking-Fundamentals/2/Resources/logfile>

### **Instructions**

1. Open the log file provided. Note that this log file contains multiple log records. Each log record is distinguished by title: Log Record 1, Log Record 2, etc.
2. Convert the binary data of each log record into a readable format with a web tool of your choosing.
   * [Convert Binary to String | Online Tool | String Functions (string-functions.com)](https://string-functions.com/binary-string.aspx)
3. Document which protocol is used for each log record.  
   * Use the following format to document the protocol for each log record: Log Record 1 = SSH.

Log Record 1 = GET / HTTP/1.1

Host: widgets.com

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.117 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9,nb;q=0.8

Log Record 2 = File Transfer Protocol (FTP)

230 Login successful.\r\n

Response code: User logged in, proceed (230)

Response arg: Login successful.

Log Record 3 =TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 56

Encrypted Application Data: d03ff41452da9e9c3ec76cbeb35e8ffc1f64bf80f512924a?

Log Record 4 =Domain Name System (query)

Transaction ID: 0x18b6

Flags: 0x0100 Standard query

0... .... .... .... = Response: Message is a query

.000 0... .... .... = Opcode: Standard query (0)

.... ..0. .... .... = Truncated: Message is not truncated

.... ...1 .... .... = Recursion desired: Do query recursively

.... .... .0.. .... = Z: reserved (0)

.... .... ...0 .... = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

applegate.com: type A, class IN

[Response In: 623]

Log Record 5 =Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Technico\_65:1a:36 (88:f7:c7:65:1a:36)

Sender IP address: 10.0.0.1

Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)

Target IP address: 10.0.0.6

#### **Bonus**

* Interpret the Bonus Log Record to determine which protocol is being used.

Log Bonus =

HCI H4

[Direction: Unspecified (0xffffffff)]

HCI Packet Type: HCI Command (0x01)

HCI Command - Read Local Supported Features

Command Opcode: Read Local Supported Features (0x1003)

Parameter Total Length: 0

[Response in frame: 4]

[Command-Response Delta: 4.181ms]