**Annex D to**

**USCP ITT**

**Course Title:** Network and Web Forensics

**University:** Edinburgh Napier University

**Location:** Edinburgh

**Proposed Number of Courses per Year:** Two

**Duration:** 1 day

**Max/Min No of Students: Max: 20 Min: 4**

**Courses Objectives:**

*The main objectives of this course are to:*

* Understand how networking protocols work over computer networks, including for network switches and routers.
* Analyse real-life network traces for a range of applications, including for Web transfers, File Transfer, and Remote Login.
* Understand the basic operation of encryption tunnels, and identity their setup.
* Understand the structure of Web logs, and how these are parsed for key information.

**General Description:**

There is an increasing need to analyse network traffic for its content. This might relate to detecting a range of threats, along within security investigations. It also has requirements within network debugging and fault tracing. This module aims to show the details of the key information fields related to network connection, including with the network packets and in the trace that these connections create within Web logs. The content includes:

* Introduction to Networking.
* Coverage of Ethernet, IP, TCP and Application layer protocols.
* Using of Wireshark to analyse key information elements within a network trace.
* Coverage of the structure of Web logs, and their analysis using Splunk.

**Intended Student Population:**

These could focus on those aiming to get involved within digital forensics, incident response, or security operations centres. It is relevant to those who want to understand the actual operation of networks, and the trace of information that can be gathered from network connections. In terms of practical skills, student will learn to use Wireshark filters to filter information, and find key data elements. Along with this, the module will include the usage of Splunk to analyse Web logs. Both of these tools are widely used in industry, and match well to knowledge development, along with matching to industry standards.

**Pre-Course Work:**

Any introductory material on how networks work.

**Other Comments:**

A certificate of completion will be awarded, with a test for knowledge and practical analysis.