CHFI 淺談網際犯罪偵查與電腦鑑識

啊！發生資安事件了！怎麼辦？

事故回應處理流程

事故回應處理流程
事前準備

事故回應處理流程

事前準備

偵測與分析

事故回應處理流程

偵測與分析

分級與排序

通報

事故回應處理流程

分級與排序

通報

封鎖

事故回應處理流程

通報

封鎖

鑑識調查

事故回應處理流程

封鎖

鑑識調查

清除與復原

事故回應處理流程

鑑識調查

清除與復原

事後檢討與改善

事故回應處理流程

清除與復原

事後檢討與改善

鑑識調查流程

鑑識調查流程

找出事故現場

鑑識調查流程

找出事故現場

進行初步調查

鑑識調查流程

進行初步調查

取得授權

進行緊急應變程序

鑑識調查流程

取得授權

進行緊急應變程序

扣押現場證據

鑑識調查流程

進行緊急應變程序

扣押現場證據

製作證據副本

鑑識調查流程

扣押現場證據

製作證據副本

建立保管鍊

鑑識調查流程

製作證據副本

建立保管鍊

安全保存原始證據

鑑識調查流程

建立保管鍊

安全保存原始證據

分析證據副本

鑑識調查流程

安全保存原始證據

分析證據副本

撰寫鑑識報告

鑑識調查流程

分析證據副本

撰寫鑑識報告

實機展示：Live Response 與記憶體鑑識

Thank You! 敬請指教！

SYSTEX making it happen 精誠資訊 | UCOM 恆逸資訊 教育訓練中心 Information Technology Education Center