Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL Paraguay de la gente

GESTIÓN DE INCIDENTES CIBERNÉTICOS

CLASE 5

Ing. Gabriela Ratti

Disclaimer

Todo el contenido de esta presentación es únicamente con fines didácticos y educativos. El uso indebido de las técnicas y/o conocimientos utilizadas en esta presentación puede ir en contra de las leyes nacionales e internacionales. El autor no se hace responsable por el uso del conocimiento contenido en la siguiente presentación. La información contenida debe ser utilizada únicamente para fines éticos y con la debida autorización.

Tipos de Incidentes Cibernéticos

DELITO vs. INCIDENTE

Incidentes Cibernéticos

- Acceso sin autorización al sistema o a sus datos
- Software malicioso (Malware)
- Denegación de servicios (DoS/DDoS)
- Escaneo / Fuerza Bruta
- Correo no deseado (Spam)
- Engaños (Phishing)
- Compromiso de Sistemas

Un incidente puede incluir varias categorías!

Delitos Informáticos

- Acceso indebido a datos
- Interceptación de comunicaciones
- Preparación al acceso indebido a datos
- Alteración de datos
- Acceso indebido a sistemas informáticos
- Sabotaje a sistemas informáticos
- Falsificación de tarjetas de crédito y débito
- Estafa mediante sistemas informáticos

Ley Nro. 4439/2011

Delitos “tradicionales” cometidos a través de medios informáticos

- Pornografía infantil
- Estafa o fraude
- Acoso sexual
- Difamación y calumnia
- Amenaza
- Violación a la propiedad intelectual y piratería

Fases de la gestión de un incidente cibernético

Modelo NIST 800-61

Fase 1 - Preparación

- Roles y Responsabilidades
- Conocer los activos de información
- Medidas preventivas
- Monitoreo continuo
- Registros continuos

Responsable: la organización

Fase 2 - Detección y análisis

- Detección y notificación del 1er Indicador de compromiso
- Análisis preliminar según evidencia inicial
  - Definición de evidencia necesaria
- Compartición de evidencia
- Análisis de la evidencia

Involucrados: la organización y equipo de respuesta de incidentes (ej.: CERT-PY)

Fase 3 - Contención, Erradicación y Recuperación

- Acciones de mitigación según resultados de la Fase 2
  - Si se encontró otros indicadores de compromiso, adquirir más evidencia y volver a Fase 2
- Acciones para eliminar compromiso
- Acciones para revertir los daños del compromiso
- Comprobación de operación normal

➡ **Involucrados:** la organización y equipo de respuesta de incidentes (ej.: CERT-PY)

Fase 4 - Actividades Post-incidente

- Investigación post-incidente (quién fue, qué falló, responsables, …)
- Acciones de mejora para la prevención
- Informe e incorporación de lecciones aprendidas

Involucrados: la organización, proveedores, organismos de aplicación de ley (ej.: Fiscalía)

RECOLECCIÓN Y ADQUISICIÓN DE EVIDENCIA DIGITAL

ISO/IEC 27037

Directrices para la identificación, recolección, adquisición y preservación de las evidencias digitales.

- Recolección: proceso de recopilación de los elementos físicos que pueden contener una potencial evidencia digital
- Adquisición: proceso de creación de una copia de datos dentro de un conjunto definido. El resultado de una adquisición es la copia de una evidencia digital

Existen 2 tipos de recolección y adquisición: de dispositivos encendidos (caliente) y de dispositivos apagados (frío)

Ver **RFC 3227**

Recolección en dispositivos encendidos

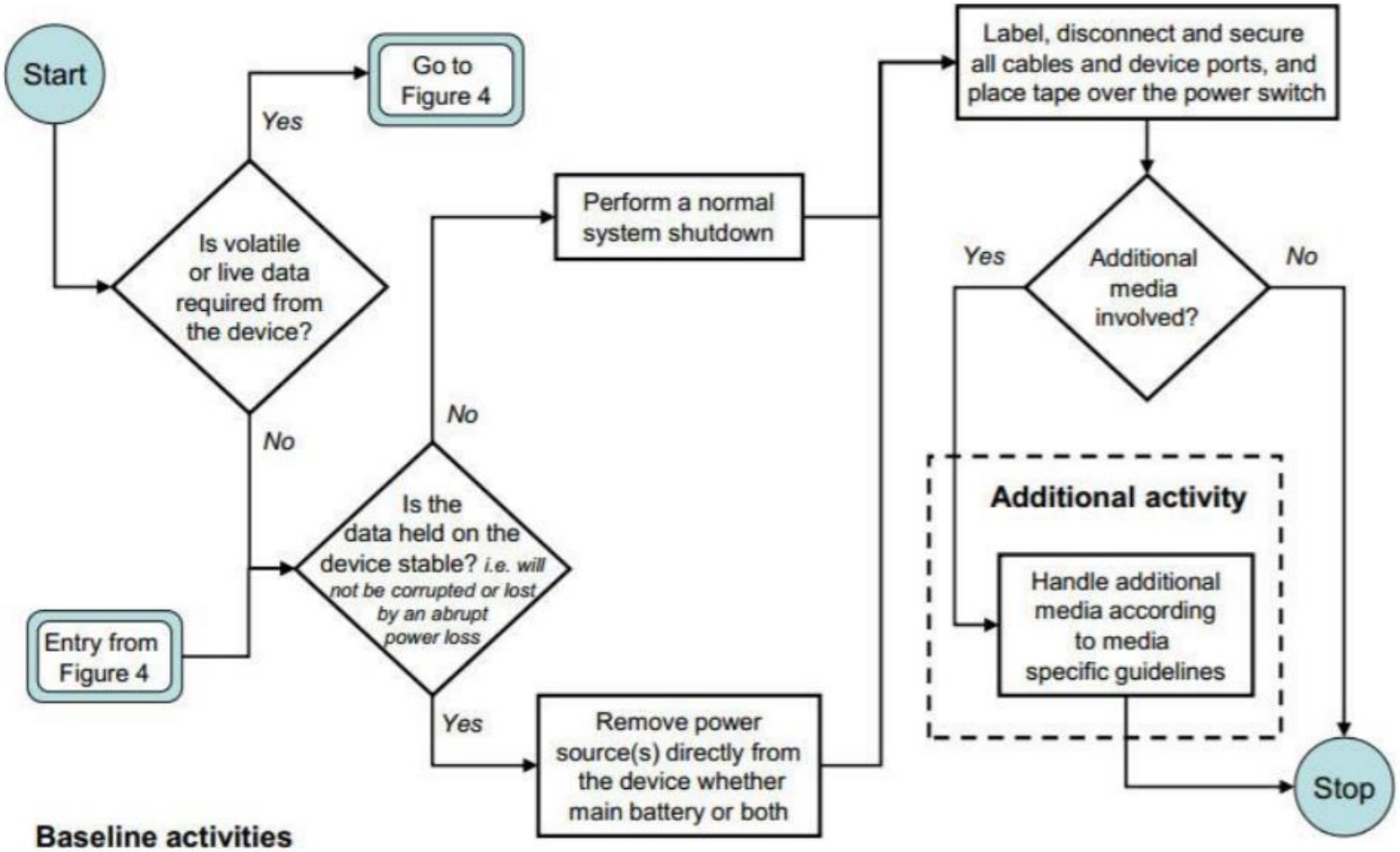

Figure 2 – Guidelines for collection of powered on digital device

Recolección en dispositivos apagados

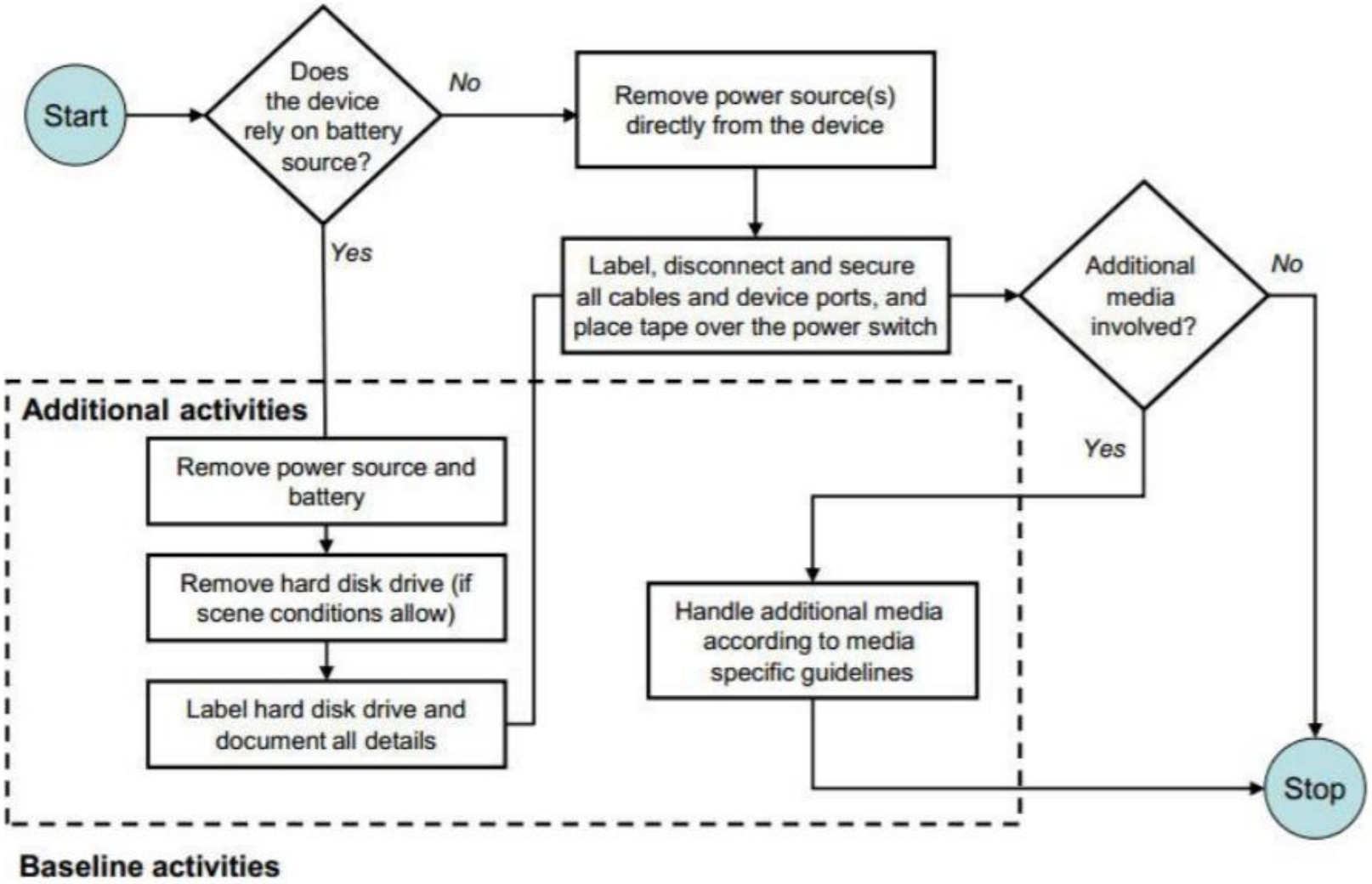

Figure 3 – Guidelines for collection of powered off digital device

Adquisición en dispositivos encendidos

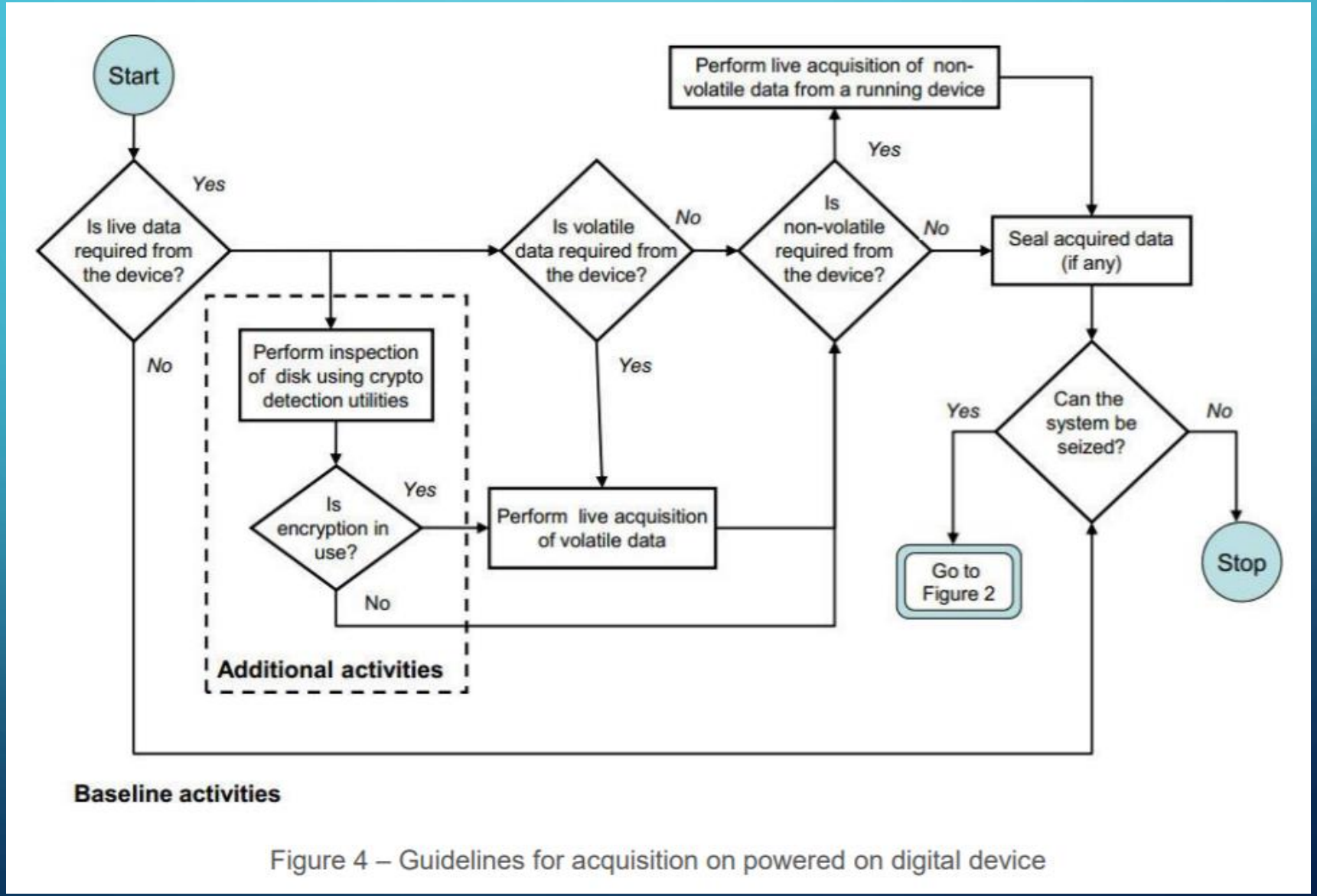

Figure 4 – Guidelines for acquisition on powered on digital device

Adquisición en dispositivos apagados

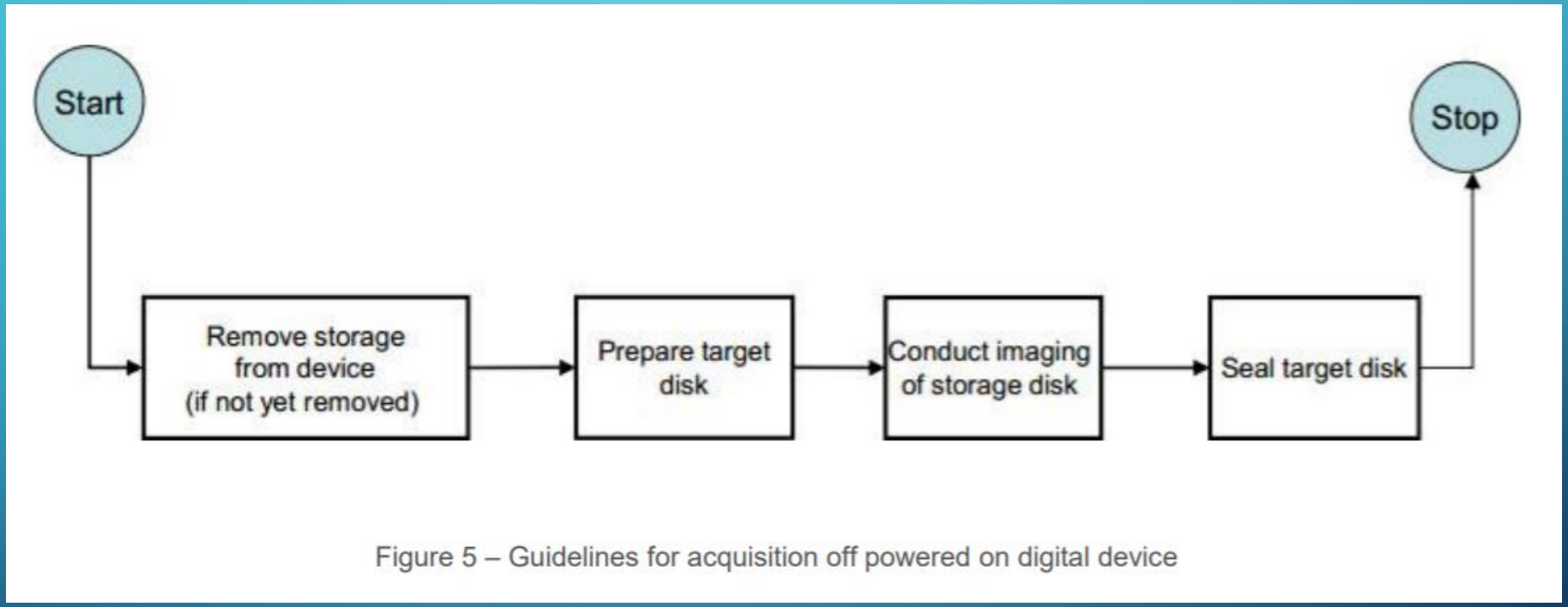

Figure 5 – Guidelines for acquisition off powered on digital device

Clonado vs imagen

- Una imagen forense es una copia exacta de un dispositivo físico que es almacenada en un archivo, el cual puede ser almacenado en cualquier tipo de dispositivo capaz de almacenar archivos.
- Por su parte, un clonado es una copia “bit a bit” de un dispositivo físico en otro dispositivo físico similar. De esta forma, el dispositivo original y el dispositivo clonado son idénticos en cuanto a contenido.

Clonado vs imagen

Imagen forense	Clonado
La copia del dispositivo origen es almacenada en un archivo.	En un dispositivo clon, la información es almacenada exactamente igual que en el dispositivo origen.
Pueden almacenarse en un único dispositivo de almacenamiento destino, archivos de imagen correspondientes a la copia de varios dispositivos de almacenamiento origen.	Cada dispositivo destino solo puede ser el clon de un único dispositivo origen. El dispositivo destino debe ser del mismo tamaño o mayor que el dispositivo origen.
Es necesario el uso de software específico para visualizar el contenido de la imagen generada.	No es necesario el uso de ningún software específico para visualizar el contenido del dispositivo clon.

Clonado vs imagen

- Adquisición física: toda la información contenida en el disco se copia exactamente igual del origen al destino. (Ej: MBR, particiones, sectores sin uso y espacio sin particionar)
- Adquisición lógica: se copia solamente un número de volumenes o una parte del mismo (Ej: conjunto de archivos o carpetas, base de datos concreta, etc.)

Evidencias según el tipo de incidente (I)

- Acceso sin autorización al sistema o a sus datos:
  - Logs a nivel de aplicación (acceso, transacción, error, etc.)
  - Logs de acceso del sistema operativo (SSH, RDP, consola, ...)
- Compromiso de Sistemas:
  - Imagen de memoria del equipo
  - Imagen de sistema de archivos del equipo
  - Logs a nivel de sistema operativo y aplicación
  - Logs y/o captura de tráfico a nivel de red (proxy, DNS, borde)
- Software malicioso (Malware):
  - Muestra del malware (el binario y sus componentes)
  - Imagen de memoria del equipo comprometido

Evidencias según el tipo de incidente (II)

- Correo no deseado (Spam):
  - Logs de servidor de correo (generación de correo)
  - Cabecera del correo (recepción de correo)
- Engaños (Phishing):
  - Cabecera del correo electrónico
  - Enlace
- Denegación de servicios (DoS/DDoS):
  - Captura de tráfico en el sistema afectado:
    - Enlace y Capa 2/3: en el router de borde y/o ISP
    - Aplicación: en el servidor

Puntos de entrada para compromiso de cuentas

Acceso indebido a nivel de capa de aplicación - correo electrónico, redes sociales, sistema interno, base de datos:

- Contraseña fácil
- Phishing
- Malware (keylogger)
- Vulnerabilidades

Puntos de entrada para software malicioso

- Acción de un usuario - Ingeniería social
  - Correo electrónico
  - Instalación manual (intencionada o no intencionada)
  - Medio físico (USB, disco duro externo, …)
- Explotación de vulnerabilidad:
  - remota, de servicio expuesto a Internet
  - local, mediante máquina comprometida en la red
  - local, mediante Drive-by Download
- Implantación mediante máquina comprometida en la red (PtH, robo de contraseña, …)
- Implantación mediante Supply-Chain attack

CASOS PRÁCTICOS

Caso Práctico 1: Phishing

El responsable del Dpto. Contable de una empresa, recibe un supuesto email de su jefe en el cual se autoriza el pago de 50.000USD a un cliente. Adjunto a dicho email, se reenvía el correo del supuesto cliente con todos los datos de pago.

El receptor de este correo, al ver el origen del mismo y el lenguaje utilizado, similar al utilizado en este tipo de comunicaciones por su superior, decide proceder al pago de dicha cantidad provocándole a la empresa una importante pérdida económica.

Caso Práctico 1: Phishing

- Emails y mensajes recibidos
- Historial de navegación
- Extensiones navegador maliciosas
- Virus / Malware

Caso Práctico 2: Acceso indebido a cuenta

El responsable de IT de una empresa, decide acceder al calendario y a los correos electrónicos del Director ejecutivo de la misma, ya que piensa que están plantándose su despido.

Para ello, puesto que la empresa hace uso de los sistemas en la nube de Microsoft, decide hacer una delegación del correo electrónico de su superior, lo que le permite recibir y responder a mensajes y convocatorias de reunión y respuestas en su nombre.

Caso Práctico 2: Acceso indebido a cuenta

- Logs de acceso y delegación
- Cambios de contraseña
- Bandejas del correo electrónico
- Virus / Malware

Caso Práctico 3: Compromiso de servidor web

La IP del servidor web de una empresa aparece una una lista negra, debido a que se detectó el envío de spam desde la misma.

El servidor web aloja únicamente la página web de la empresa. Se sospecha que el servidor se encuentra comprometido

Caso Práctico 3: Compromiso de servidor web

- Logs de acceso (ssh, rdp, ftp, etc.)
- Logs de aplicación (http, smtp)
- Virus / Malware:
  - Sistema de archivos (disco duro)
  - Procesos, conexiones (RAM)

Caso Práctico 4: Fuga de información

Un empleado descontento decide obtener unos ingresos extra pasando información confidencial de su actual empresa a la competencia. Dicha información incluye presupuestos y expedientes de concursos en los cuales, su actual empresa está participando.

Para enviar toda la información, el usuario hace uso de su cuenta de correo personal, no vinculada a la empresa.

Caso Práctico 4: Fuga de información

- Logs de acceso / aplicación
- Bandejas del correo electrónico
- Logs del sistema operativo
- Virus / Malware:
  - Sistema de archivos (disco duro)
  - Procesos, conexiones (RAM)

Caso Práctico 5: Clonación de tarjetas

Múltiples clientes de un banco empiezan a reportar extracciones de dinero no reconocidas de sus cuentas.

El banco analiza las actividades de dichas cuentas y encuentra que, días previos, todas habían realizado transacciones en un mismo cajero, por lo que sospecha que el mismo puede estar comprometido

Caso Práctico 5: Clonación de tarjetas

- Logs de transacciones bancarias
- Dispositivo físico para clonación (skimmer)
- Grabaciones de CCTV

Caso Práctico 6: Vaciamiento de cajero

Un banco observa que un cajero indica un nivel insuficiente de billetes. Al verificar el cajero, se observa que el mismo se encuentra vacío. Sin embargo, la suma de las extracciones de clientes es inferior al monto de dinero que había en el cajero.

Caso Práctico 6: Vaciamiento de cajero

- Logs de transacciones bancarias
- Grabaciones de CCTV
- Virus / Malware:
  - Sistema de archivos (disco duro)
  - Procesos, conexiones (RAM)

MUCHAS GRACIAS!

Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN