

The banner features a dark blue background with a perspective view of a hallway lined with server racks. The racks are illuminated from within, and a bright light source is visible at the end of the hallway. The text "VIII Jornada Nacional de Seguridad Informática" is written in a bold, yellow, sans-serif font.

**VIII Jornada Nacional de
Seguridad Informática**



Aplicaciones forenses del NTP En busca del tiempo perdido

Introducción

- Principio fundamental de las ciencias forenses
- Dr. Edmon Locard
- Principio de intercambio en el ciberespacio.
- Los sistemas deben ser preparados adecuadamente.
- Bitácora del sistema.

NTP

- Dr. Davis Mills.
- Funcionamiento.
- Sincronización.
- Filtro de Mínima.

Uso de NTP en Forense

- Incluso máquinas homogéneas requieren un mecanismo de sincronización.
- 3 Tipos de sincronización.
- En ambientes seguros se recomienda tener un servidor NTP.

Hora real de un evento

- 74 % de Host con un rango de 10s.
- 26 % rangos mayores.
- 50% < 1s.
- Ordenar temporalmente los hechos.

Técnica propuesta

- Análisis *post-mortem* de los *logs*.
- Establecer reloj de referencia.
- Conocer el desfase de la hora y la deriva de la frecuencia.
- Recalcular todas las estampas de tiempo a una hora común.
- Establecer el orden de ocurrencia de los eventos.

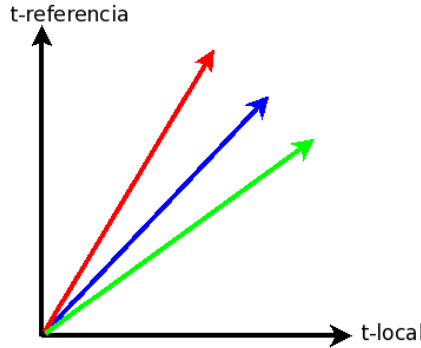
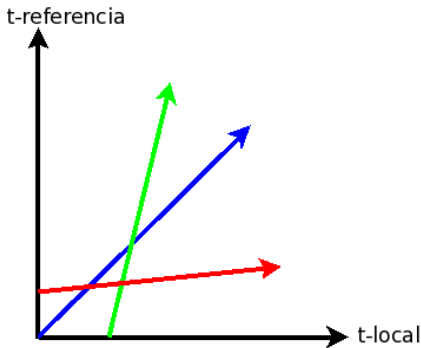
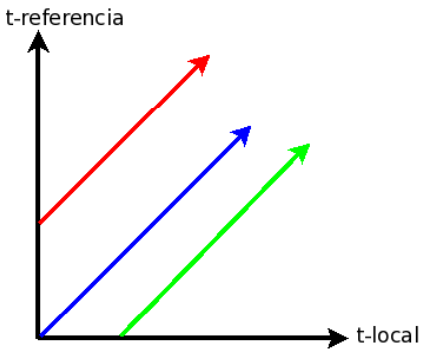
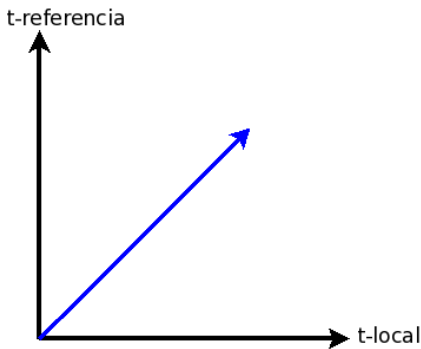
Casos del Reloj

$$y = x$$

$$y = x + b$$

$$y = mx$$

$$y = mx + b$$



- Tiempo de referencia
- ↑ Tiempo local de la maquina
- Maquina sincronizada
- Maquina local no sincronizada 1
- Maquina local no sincronizada 2

Obtener desfase de tiempo y frecuencia

- Desplazamiento: `ntpdate`
- Deriva:
 - `ntptime -f 0`
 - Configurar `ntp` para que se sincronice con un servidor confiable.
 - Eliminar `ntp.drif`.
 - Ejecutar *daemon* y esperar a que `ntpq -c rv presente status=4` y obtener la deriva del campo *frequency*.

- Si m es la deriva,
entonces.

$$m \approx 1 + f$$

Para calcular b se procede de la siguiente manera:

VIII Jornada Nacional de Seguridad Informática



Sea:

$$\left\{ \begin{array}{l} o : \text{desplazamiento,} \\ x = t \end{array} \right\}$$

$$y = tm + b$$

$$y = t + o$$

$$t + o = tm + b$$

$$b = t(1 - m) + o$$

$$b = t(-f) + o$$

Una vez calculado m y b y sea t_n
Se desea calcular t'_n

$$t_n = mt'_n + b$$

$$t'_n = \frac{t_n - b}{m} = \frac{t_n - t(-f) - o}{1 + f}$$