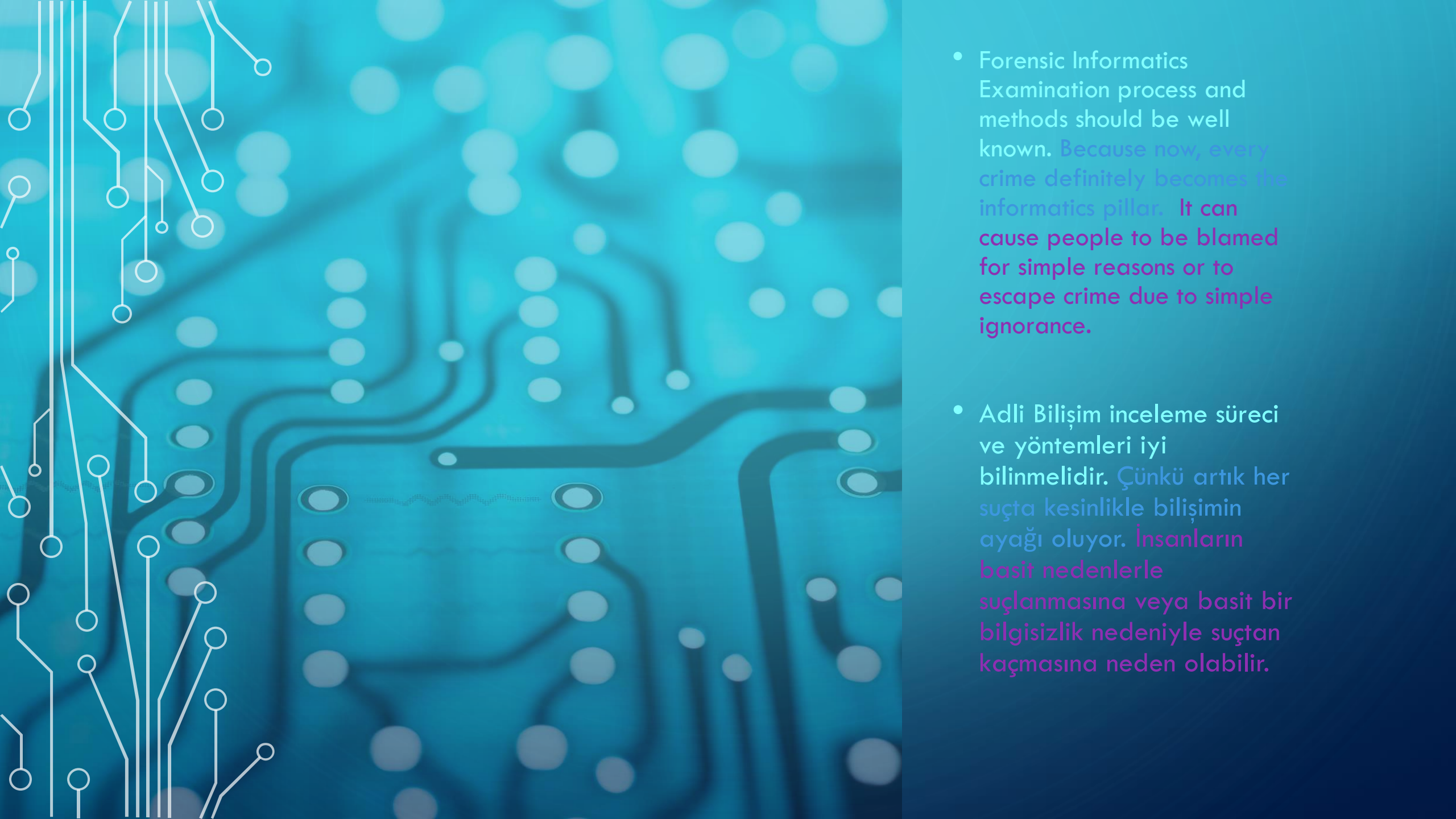


# COMPUTER FORENSIC EXAMINATION PROCESS AND METHODS

-ERHAN BARAN-

- 
- Forensic Informatics Examination process and methods should be well known. Because now, every crime definitely becomes the informatics pillar. It can cause people to be blamed for simple reasons or to escape crime due to simple ignorance.
  - Adli Bilişim inceleme süreci ve yöntemleri iyi bilinmelidir. Çünkü artık her suçta kesinlikle bilişimin ayağı oluyor. İnsanların basit nedenlerle suçlanmasına veya basit bir bilgisizlik nedeniyle suçtan kaçmasına neden olabilir.







# DEFİNİTİON

- Forensic Informatics Examination Identification process begins with the identification and collection of potential data storage resources to be examined. Typical data sources are hard disks mounted on computers, CD, DVD, USB disks, flash disks, memory cards, floppy disk, GPS, mobile phone. Are the resources limited to this? Of course not. Data such as a magnetic card copier, a database application, a website logs, a phone call traffic can also be the source.
- Adli Bilişim İncelemesi Tanımlama süreci, incelenecek potansiyel veri depolama kaynaklarının tanımlanması ve toplanmasıyla başlar. Bilgisayarlara takılı sabit diskler, CD, DVD, USB diskler, flash diskler, hafıza kartları, disket, GPS, cep telefonu tipik veri kaynaklarıdır. Kaynaklar bununla sınırlı mı? Tabii ki değil. Manyetik kart kopyalayıcı, veritabanı uygulaması, web sitesi günlükleri, telefon görüşmesi trafiği gibi veriler de kaynak olabilir.

# EXAMINATION

- Making exact copies of the collected data sources and conducting the research on these copies is the process of examination. **It is essential to protect the data integrity of the evidence examined here. In other words, the evidence should be preserved from the moment the evidence is seized.** The processes of collecting data from a working computer and a closed computer are different. In this narrative, the default is an intervention on a closed computer.
- Toplanan veri kaynaklarının birebir kopyalarının çıkarılması ve bu kopyalar üzerinde araştırma yapılması inceleme sürecidir. **Burada incelenen kanıtların veri bütünlüğünü korumak esastır. Diğer bir deyişle, delil ele geçirildiği andan itibaren delil korunmalıdır.** Çalışan bir bilgisayardan ve kapalı bir bilgisayardan veri toplama işlemleri farklıdır. Bu anlatımda varsayılan, kapalı bir bilgisayara yapılan müdahaledir.



# REPORTING

- The process by which the information obtained during the analysis process is presented is the reporting process. Reporting should be clear and clear to the reader and should include evaluations rather than claims. Of course, these 4 processes listed above are widely applied. **The process can be flexible according to the resources defined. For example, in a system with 1000-2000 clients, it is not a practical solution to make exact copies of all computers in the system.** Or, again, it doesn't make sense to shut down the whole system to examine a database application that thousands of clients use. Therefore, the intervention method will change according to the characteristics of the systems. Perhaps no exact copies of some resources will be obtained, the examination will be made while the system is running.
- Analiz sürecinde elde edilen bilgilerin sunulduğu süreç raporlama sürecidir. Raporlama okuyucu için açık ve net olmalı ve iddialar yerine değerlendirmeleri içermelidir. Elbette yukarıda sıralanan bu 4 işlem yaygın olarak uygulanmaktadır. **Bu süreç, tanımlanan kaynaklara göre esnek olabilir. Örneğin 1000-2000 istemcili bir sistemde, sistemdeki tüm bilgisayarların birebir kopyalarını almak pratik bir çözüm değildir. Veya yine, binlerce istemcinin kullandığı bir veritabanı uygulamasını incelemek için tüm sistemi kapatmak mantıklı değildir. Bu nedenle müdahale yöntemi sistemlerin özelliklerine göre değişecektir. Belki bazı kaynakların birebir kopyaları alınmayacaktır, inceleme sistem çalışırken yapılacaktır.**