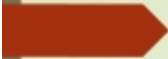



Machine Learning/Data Mining


Instructor: Chris Ding

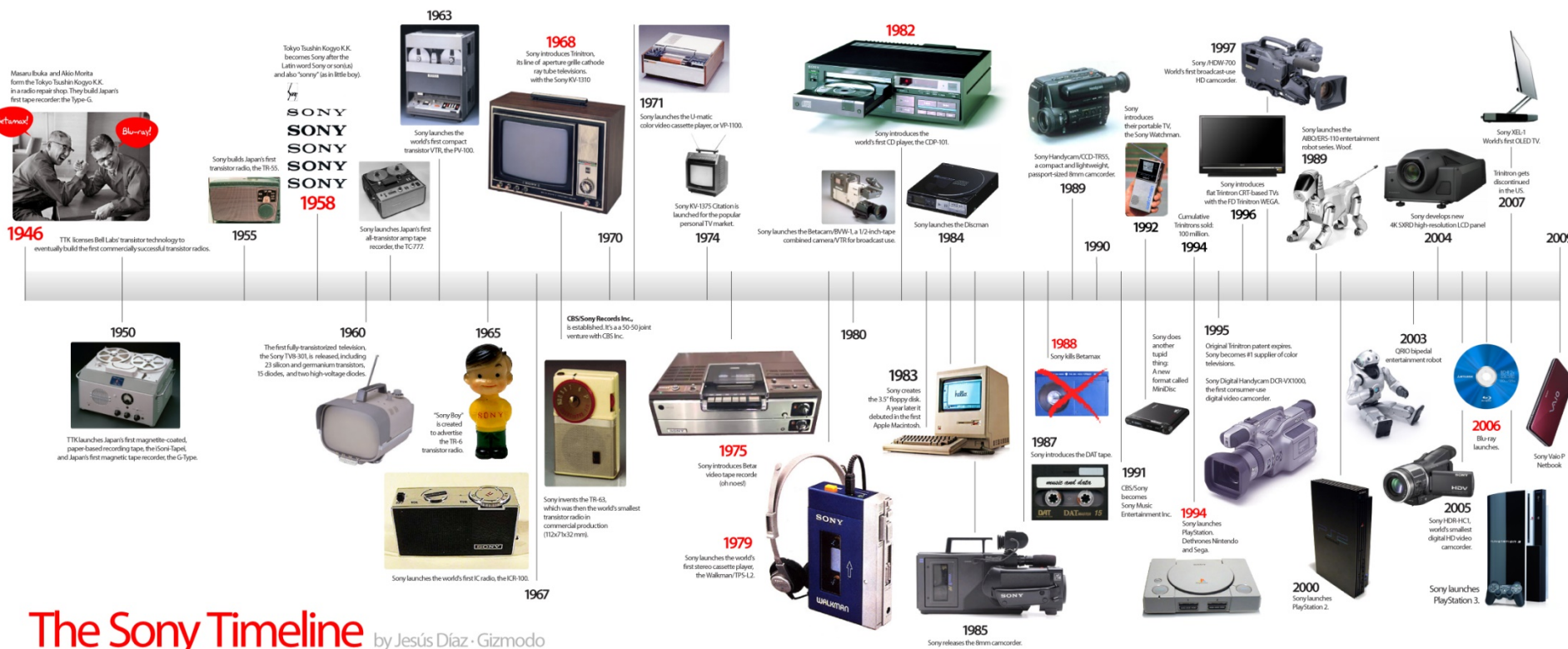
Information Technology Revolution

 Revolution

Technology (and I.T) is advanced, such as with the advent of personal computer in the 1980s and its everyday use in the home and the workplaces. The world moved into the information age. I.T changed and it has changed our lifestyle.







The Sony Timeline by Jesús Díaz · Gizmodo

Then comes the internet ---



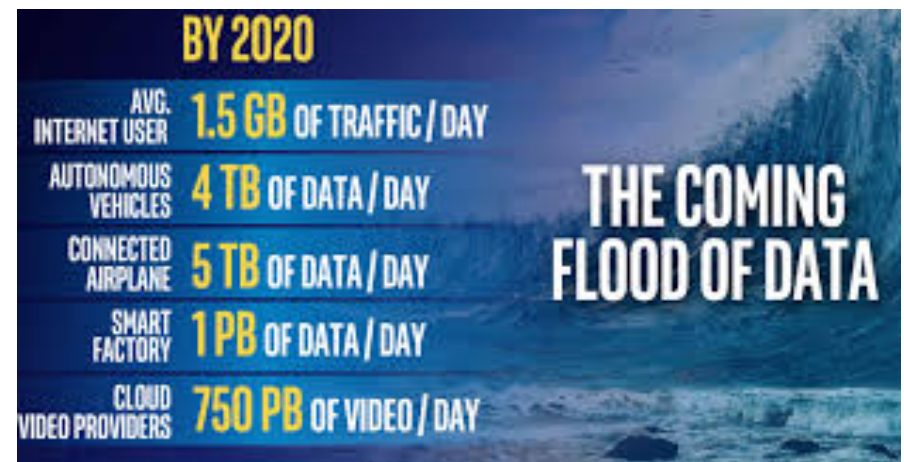
The entire world is under your fingertips





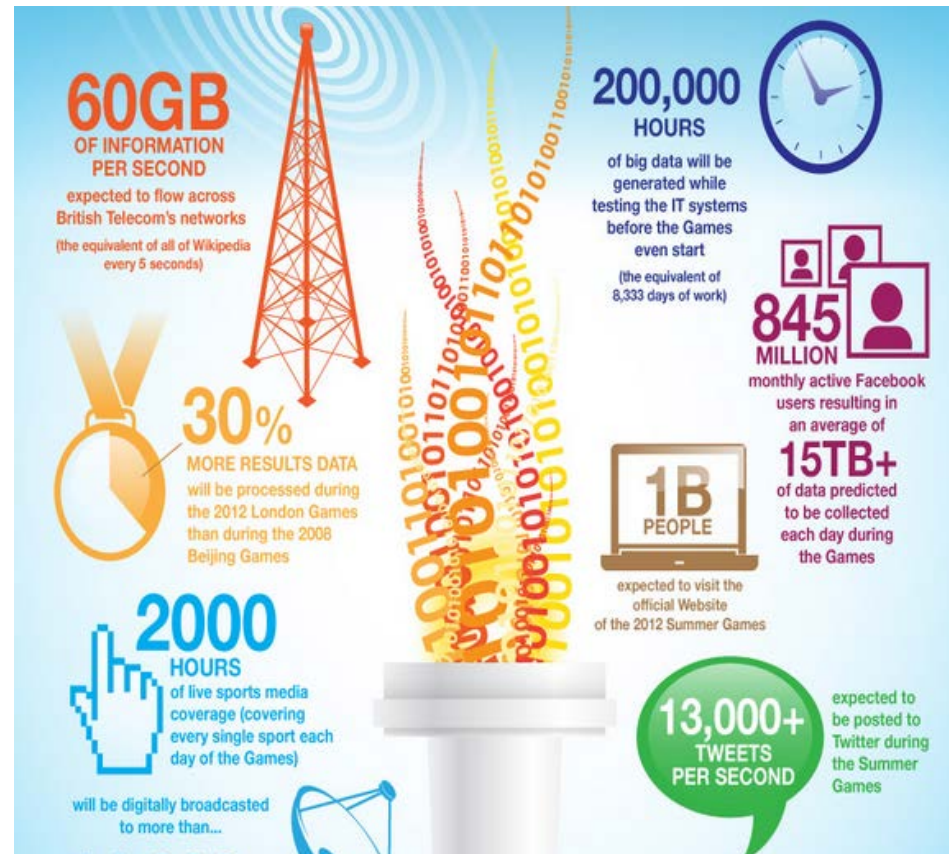
A cellphone is most powerful knowledge and communication tool/database

It uses many many data mining technology



The Unstructured Data Explosion

- Growing 100X every 10 years
- Requires a new approach



What Happens in an Internet Minute?



And Future Growth is Staggering

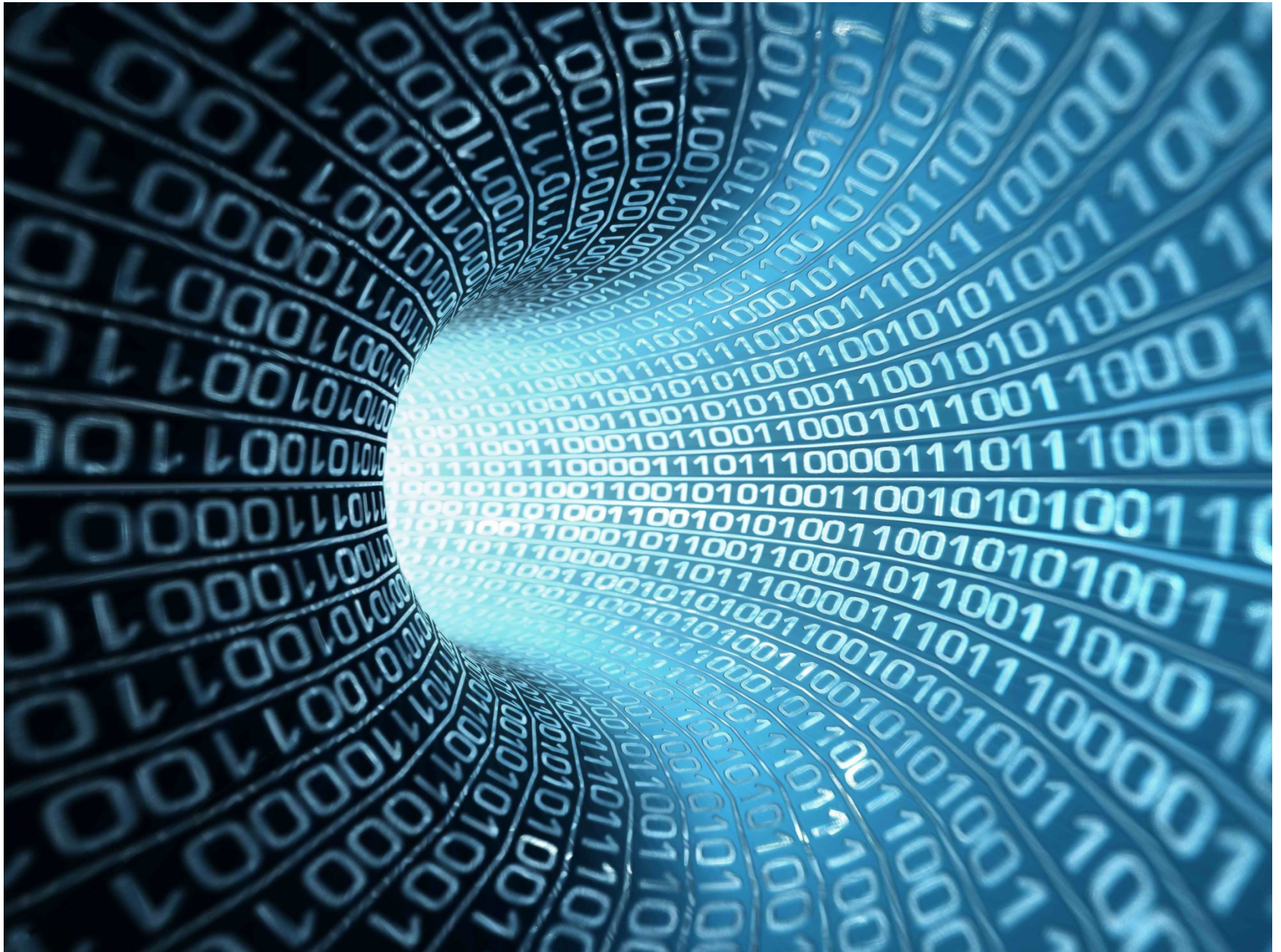




The New Technology:
data mining, machine learning, AI

Turning data into knowledge





Search Engine Google uses many data mining technology

The image is a screenshot of a Google search interface. At the top left is the Google logo. To its right is a search bar containing the text "data mining" and a magnifying glass icon. Below the search bar is a horizontal menu with tabs: "All" (selected), "News", "Books", "Images", "Videos", "More", "Settings", and "Tools". Below the menu, it says "About 55,000,000 results (0.54 seconds)".

The first search result is an advertisement for IBM. It has a green "Ad" label and a link to "www.ibm.com/PredictiveAnalytics". The title is "Data Mining - ibm.com". The description is "Data Mining Through IBM Allows For Analysis From Various Models." Below the description are two columns of links: "Platform & Technology", "IBM Analytics for Spark", "IBM Cloud Data Services", and "Advanced Analytics".

The second search result is an advertisement for SAS. It has a green "Ad" label and a link to "www.sas.com/Data-Mining/White-Papers". The title is "How Data Mining Works - Free White Paper Download - sas.com". The description is "Applying data mining and real-time analytics in oil and gas operations." Below the description are several links: "Machine Learning", "Predictive Analytics", "Business Analytics", "Statistical Analytics", "SAS Analytics Products", "Analytics White Papers", "Analytics Webinars", and "How to Buy SAS Analytics".

Below the search results is a knowledge panel for "data mining". The title "data mining" is in a large, bold, black font. Below the title is the word "noun" and a grey box containing the word "COMPUTING". Below that is the definition: "the practice of examining large databases in order to generate new information." At the bottom of the panel is a chevron icon and the text "Translations, word origin, and more definitions".

Below the knowledge panel is a link to "Data mining - Wikipedia" with the URL "https://en.wikipedia.org/wiki/Data_mining".

At the bottom right of the page is a "Feedback" link.



SPEECH
TO TEXT



Employs low latency speech recognition capabilities to convert English speech to text

TEXT TO
SPEECH



Synthesizes natural-sounding speech from text in English and Spanish

VISUAL
RECOGNITION



Analyzes the visual content of images and videos to understand their content

CONCEPT
INSIGHTS



Explores the concepts behind your input, identifying associations beyond traditional text matching

TRADEOFF
ANALYTICS



Helps users make better choices by weighing multiple and often conflicting goals

IBM Watson uses many many machine learning technology

Security. One that Watson should help mitigate.

IBM Watson™



IBM Watson Knowledge Studio

VIEW DETAILS REPLACE CONCORDANCE ATTRIBUTE VIEW

In Progress SAVE CLOSE

Alpha... 16pt 1



STEP 2: THE FIRST STAGE MALWARE IS EXECUTED

Once the Upatre malware is executed, its sole purpose is to download Dyre.

This is completed in a few stages.

It's important to note that this stage of the process is completely dynamic.

URLs and payloads are constantly shifting in order to evade detection.

The Upatre malware itself constantly evolves and remains obfuscated, allowing it to evade antivirus measures as well.

1) Upatre contacts checkip.dyndns.org in order to determine the public IP address of the machine it is on.

This website replies with a simple message 'Current IP Address: x.x.x.x'.

The malware uses this information to understand who it has infected.

2) Next, a STUN (Session Traversal Utilities for NAT) server is contacted to determine the public IP address and the type of NAT (Network Address Translation) service it's sitting behind.

3) Internet connectivity is checked to determine if a proxy is being utilized by contacting google.com.

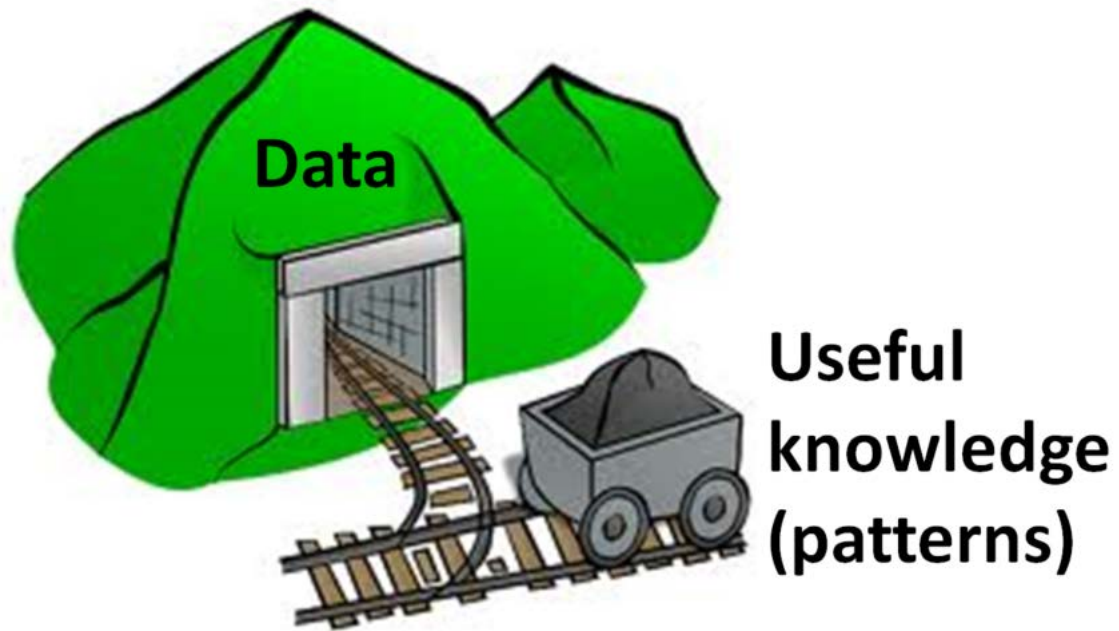
4) Upatre makes its initial contact with the Command & Control (C&C) server.

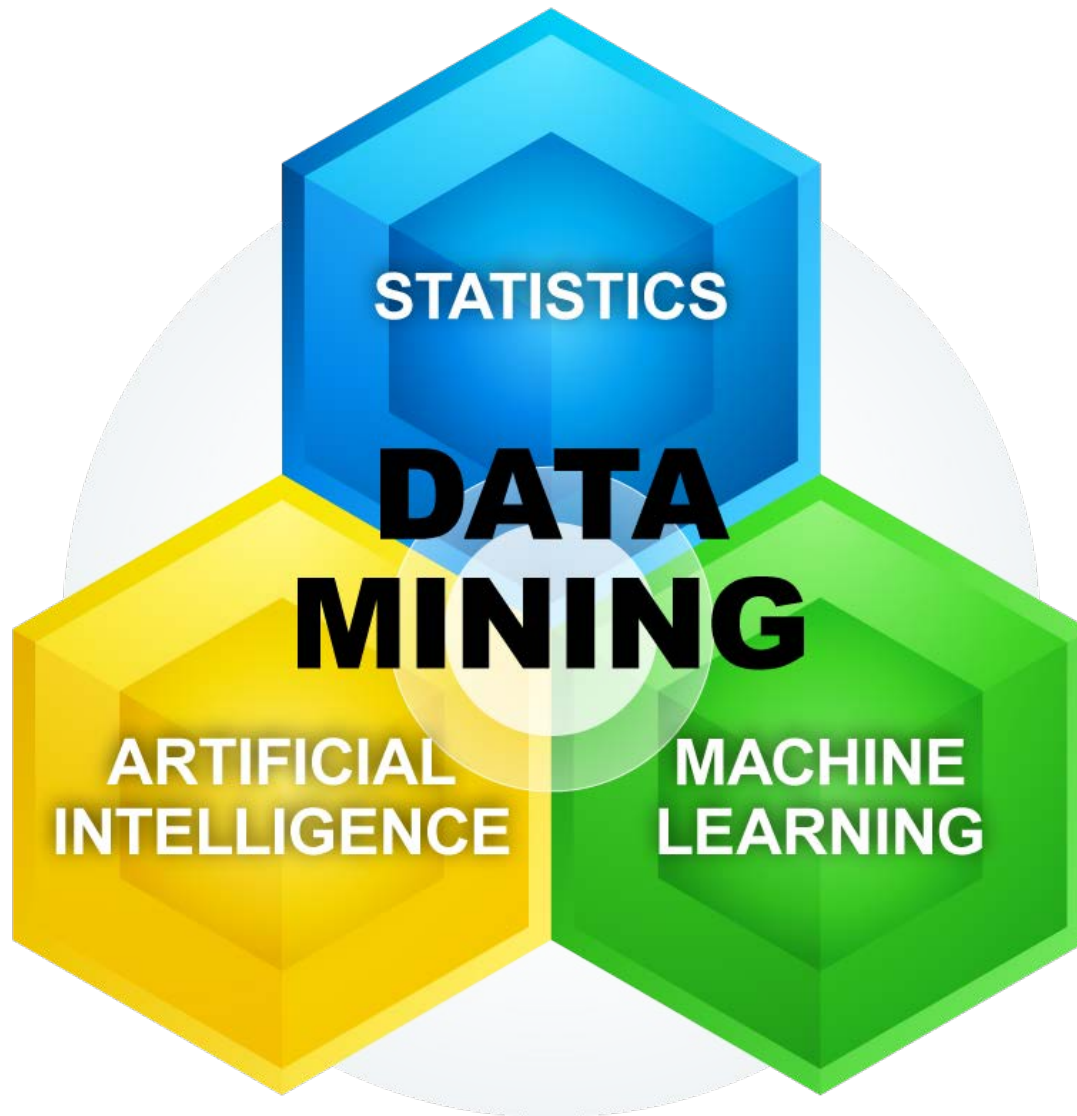
5) Upatre downloads Dyre from a variety of domains as well as executing flopper

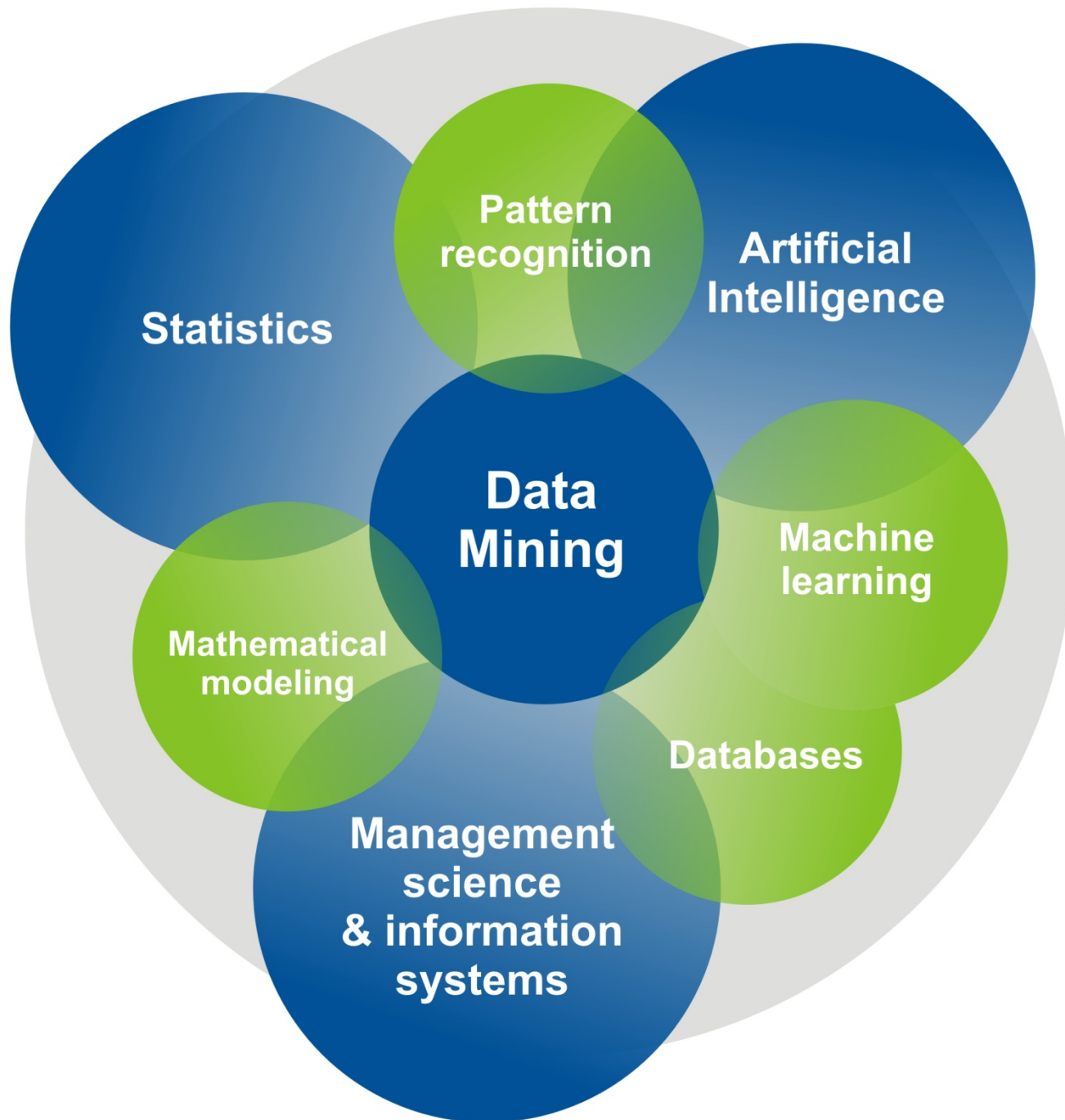
Entity			Mention		
Type	Subtype	Role			
-	ADVERSARY_RESOURCE				
c	CAMPAIGN				
r	COURSE_OF_ACTION				
e	EXPLOIT_TARGET				
g	GPE				
-	IMPACT				
d	INCIDENT				
i	INDICATOR				
-	INTENDED_EFFECT				
o	ORGANIZATION				
p	PERSON				
x	RESOURCE				
-	STATE_VARIABLE				
-	SYMPTOMS				
-	TARGET				
x	THREAT_ACTOR				



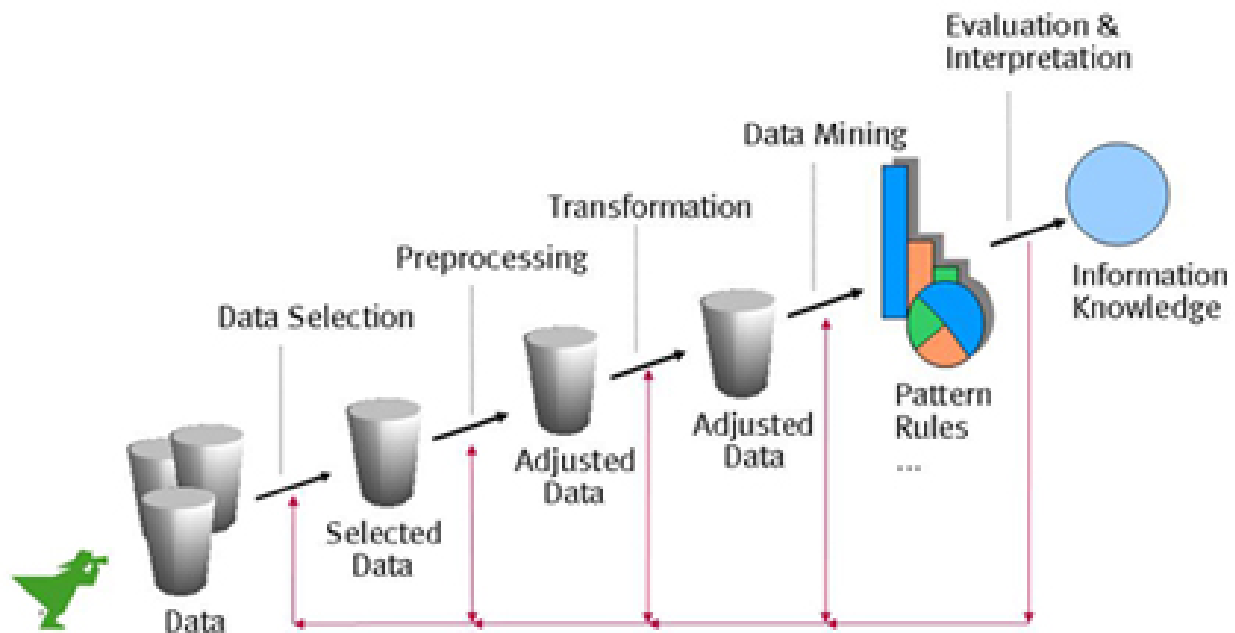
Data Mining: **extract knowledge from data**







Data Mining Model



3 Examples of Data Mining

- Market basket data
- Handwritten digits recognition
- Cancer detection from gene expression data

Market Basket Data Analysis

Market Basket Example



- ? Where should detergents be placed in the Store to maximize their sales?
- ? Are window cleaning products purchased when detergents and orange juice are bought together?
- ? Is soda typically purchased with bananas? Does the brand of soda make a difference?
- ? How are the demographics of the neighborhood affecting what customers are buying?

Market Basket Data Analysis: find associations

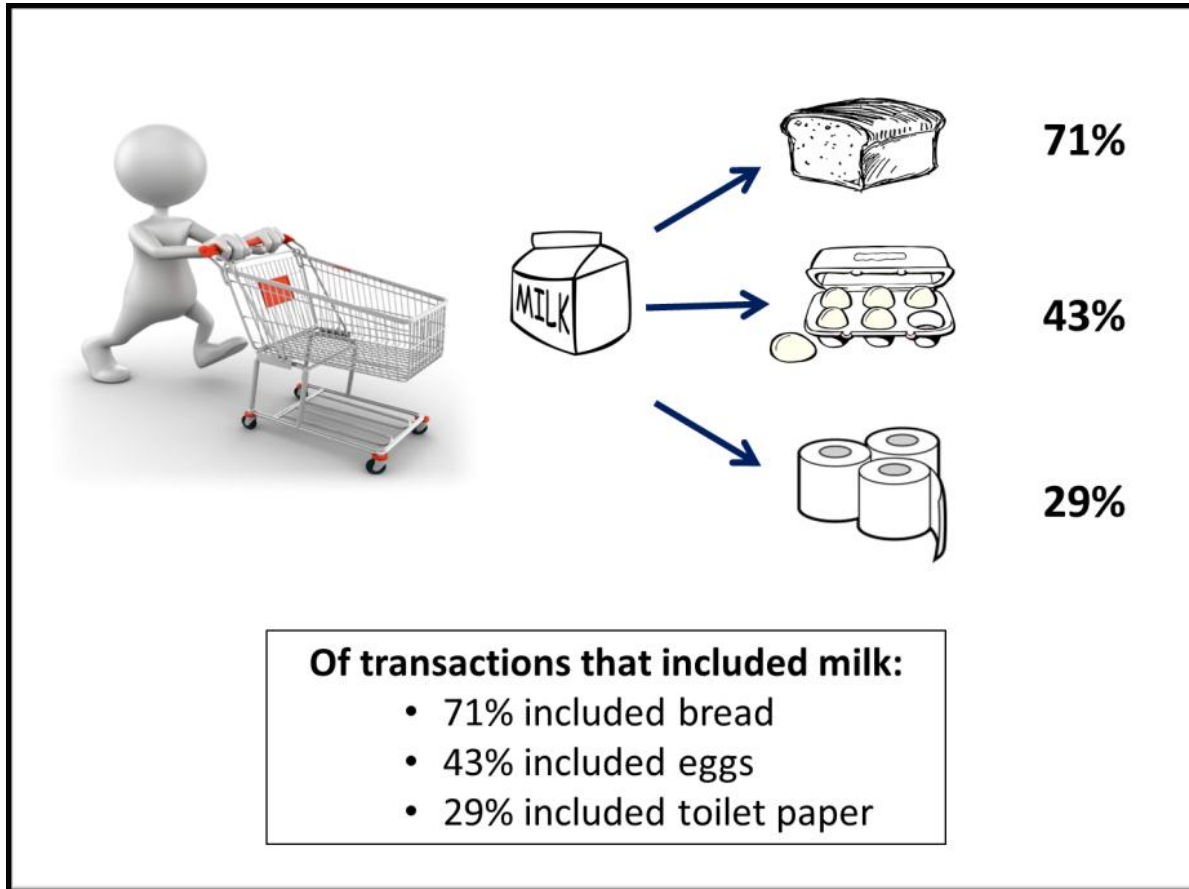


Table 1. Market basket transactions

<i>Transaction ID</i>	<i>Items Bought</i>
1	{ <i>Laptop, Printer, Tablet, Headset</i> }
2	{ <i>Printer, Monitor, Tablet</i> }
3	{ <i>Laptop, Printer, Tablet, Headset</i> }
4	{ <i>Laptop, Monitor, Tablet, Headset</i> }
5	{ <i>Printer, Monitor, Tablet, Headset</i> }
6	{ <i>Printer, Tablet, Headset</i> }
7	{ <i>Monitor, Tablet</i> }
8	{ <i>Laptop, Printer, Monitor</i> }
9	{ <i>Laptop, Tablet, Headset</i> }
10	{ <i>Printer, Tablet</i> }

Market Basket Analysis

An example of market basket transactions.

TID -- Items

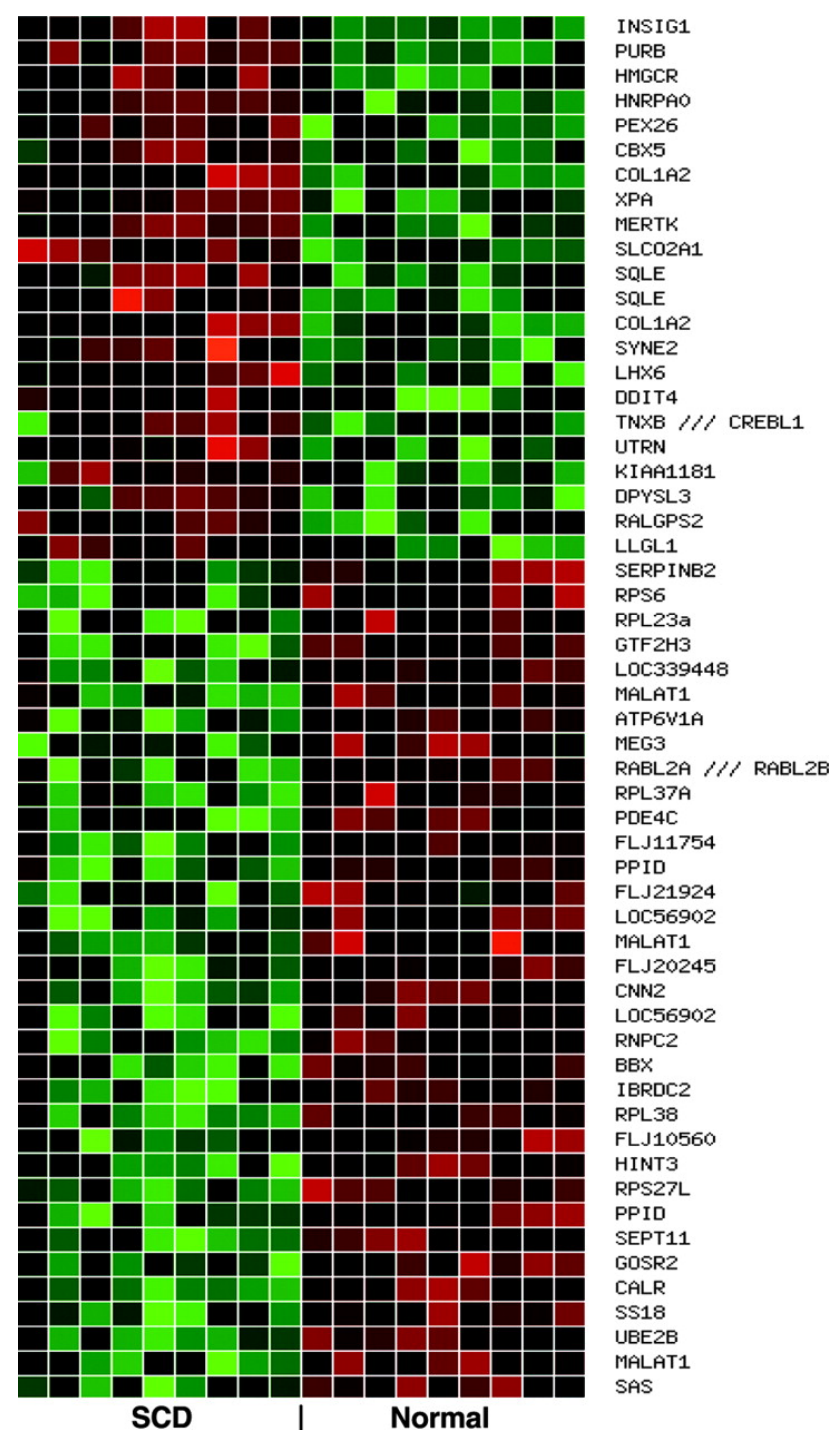
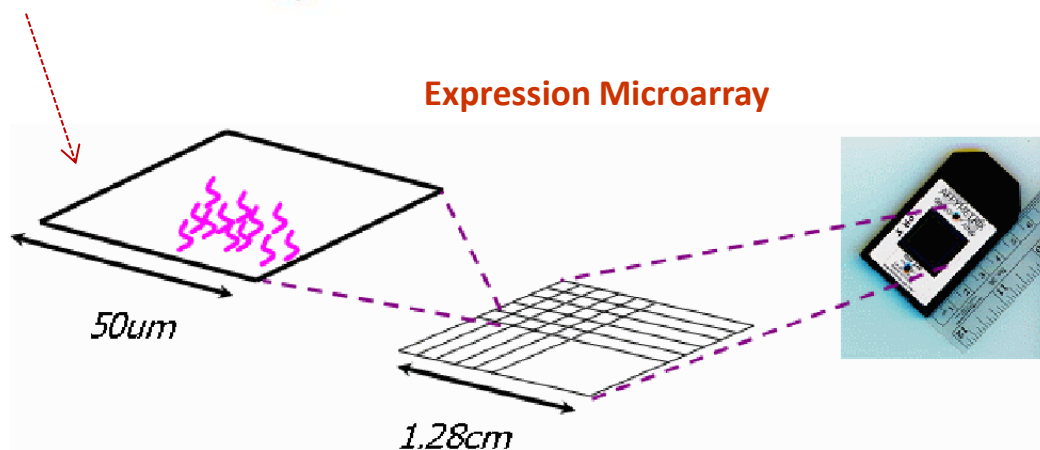
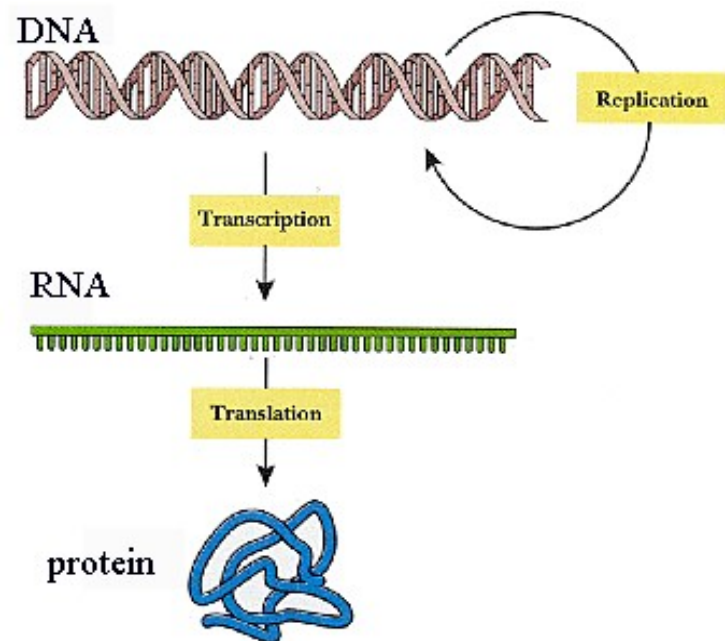
- 1.{Bread, Milk}
- 2.{Bread, Diapers, Beer, Eggs}
- 3.{Milk, Diapers, Beer, Cola}
- 4.{Bread, Milk, Diapers, Beer}
- 5.{Bread, Milk, Diapers, Cola}



WAL★MART®



DNA Gene Expressions to detect cancer



Recognize handwritten digits and letters.

All post office mailed letters are machine scanned to automatically decide the destination zip-code

