Independent AV testing

Ph.D. Ferenc Leitold

fleitold@checkvir.com

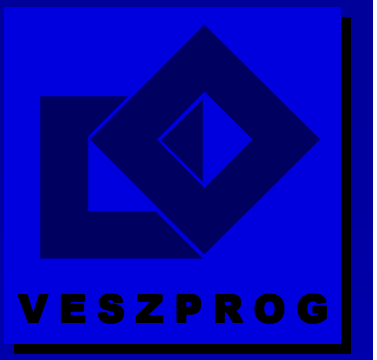
www.checkvir.com

VESZPROG Ltd.

&

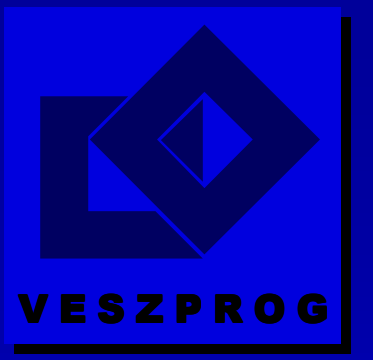
University of Veszprém

Contents



- CheckVir project
- Our viewpoint about testing
- Testing procedures
- Results

CheckVir project

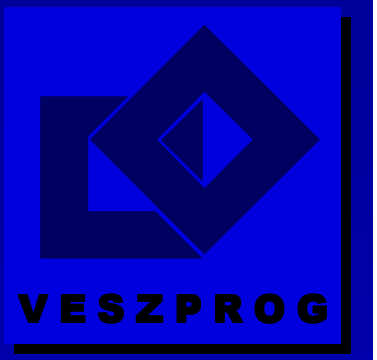


- **Main goals of AV testing**
  - Inform AV users
  - Help AV developers in their work
- **Developing automatic AV testing methods**
  - started at the end of 2000
  - supported by the *Hungarian Ministry of Education, Research and Development Division*
- **Testing plan for 2002 was announced in March 2002**
- **Increasing computing capacity by July 2002**

Our viewpoint

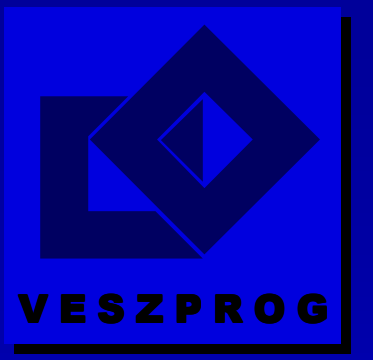
- We distinguish bugs and problems
- We do not count the correct behaviour
- We count only bugs and problems

Testing procedures



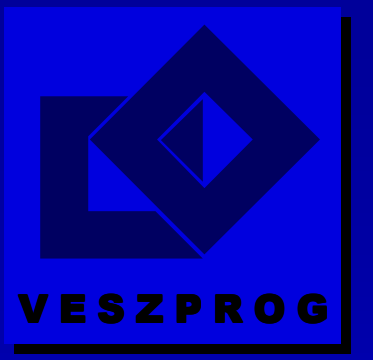
- Knowledge base tests
  - Test of scanning and disinfection
  - On-access and on-demand tests
  - Comparing the results of “different usages”
  - False positive test
  - Testing in as real environment as possible
- Checking the speed of execution
- Checking features, support, …

Knowledge base tests



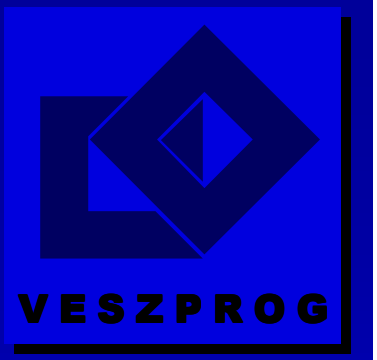
- Preparing virus samples for test
- Installing and executing AV product
- Analysing results

Virus samples



- Big number of samples should be replicated
- Test sets
  - ItW test set including old and new viruses
  - test set for testing the engine capability
- Which samples should be used ?
  - only virus samples (can infect other goats) or
  - samples modified by viruses
    (workable infection, bad infection, corrupted)

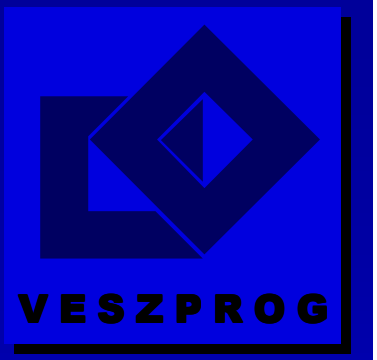
Virus samples



- Big number of samples should be replicated
- Test sets
  - ItW test set including old and new viruses
  - test set for testing the engine capability
- Which samples should be used ?
  - only virus samples (can infect other goats) or
  - samples modified by viruses
    (workable infection, bad infection, corrupted)

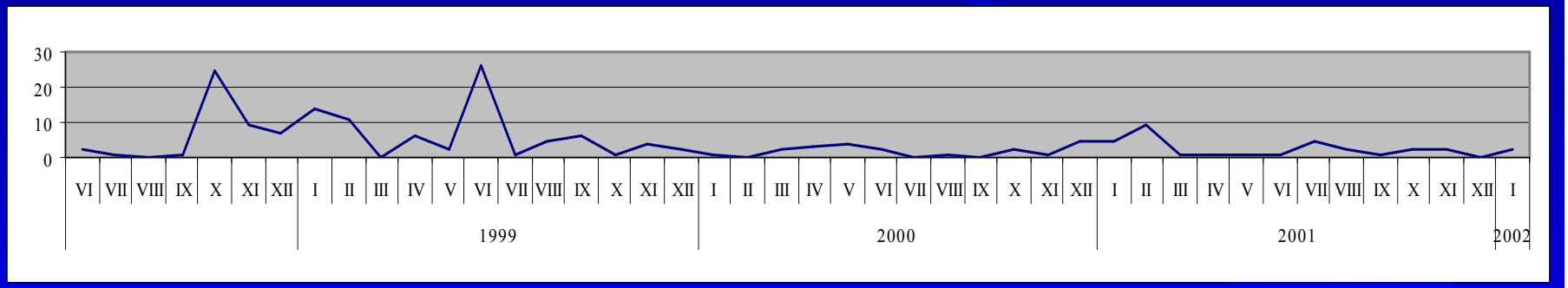
Virus samples

Why should we use old viruses ?



Virus samples

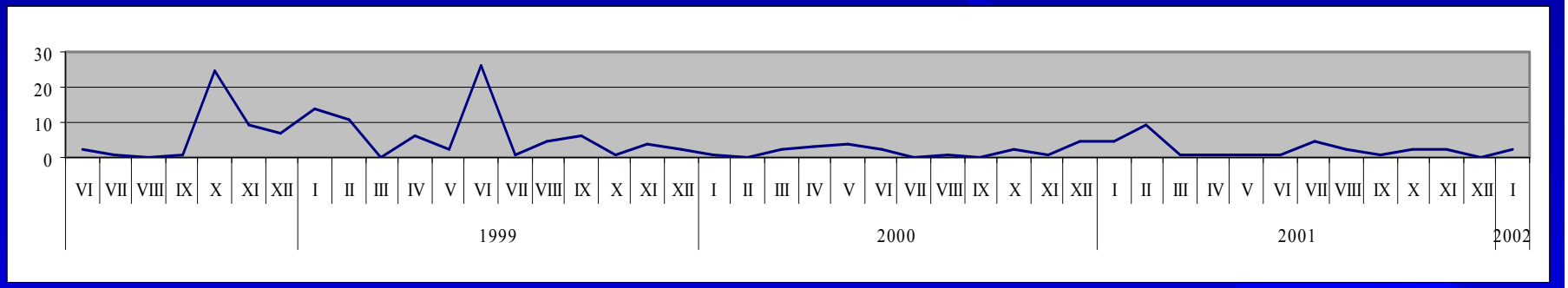
Why should we use old viruses ?

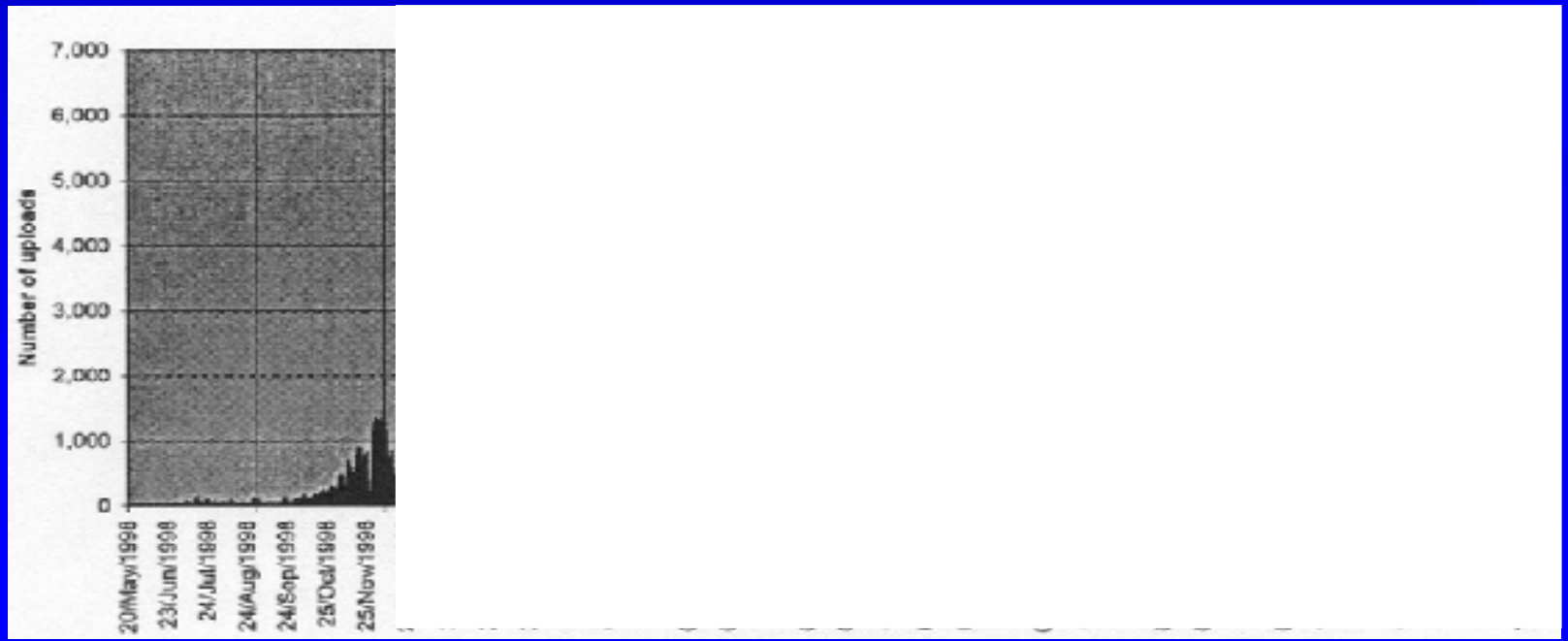


Virus samples

Why should we use old viruses ?

VESZPROG

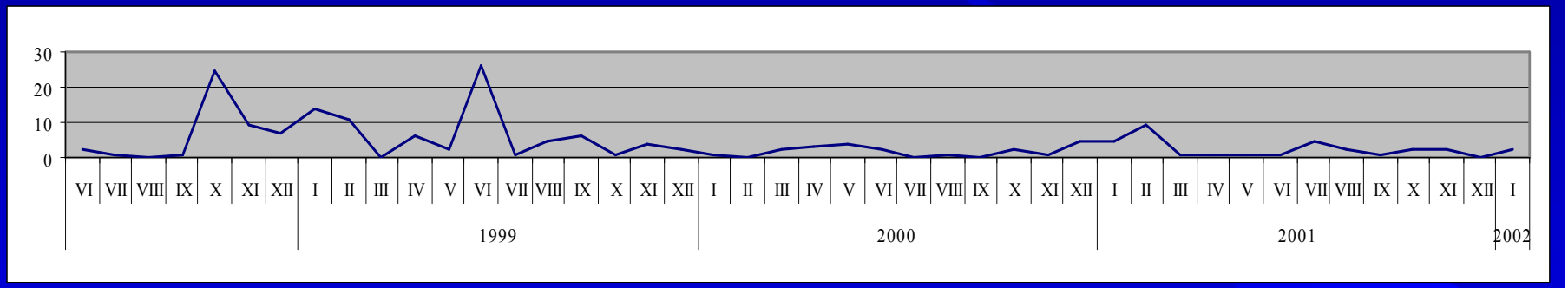


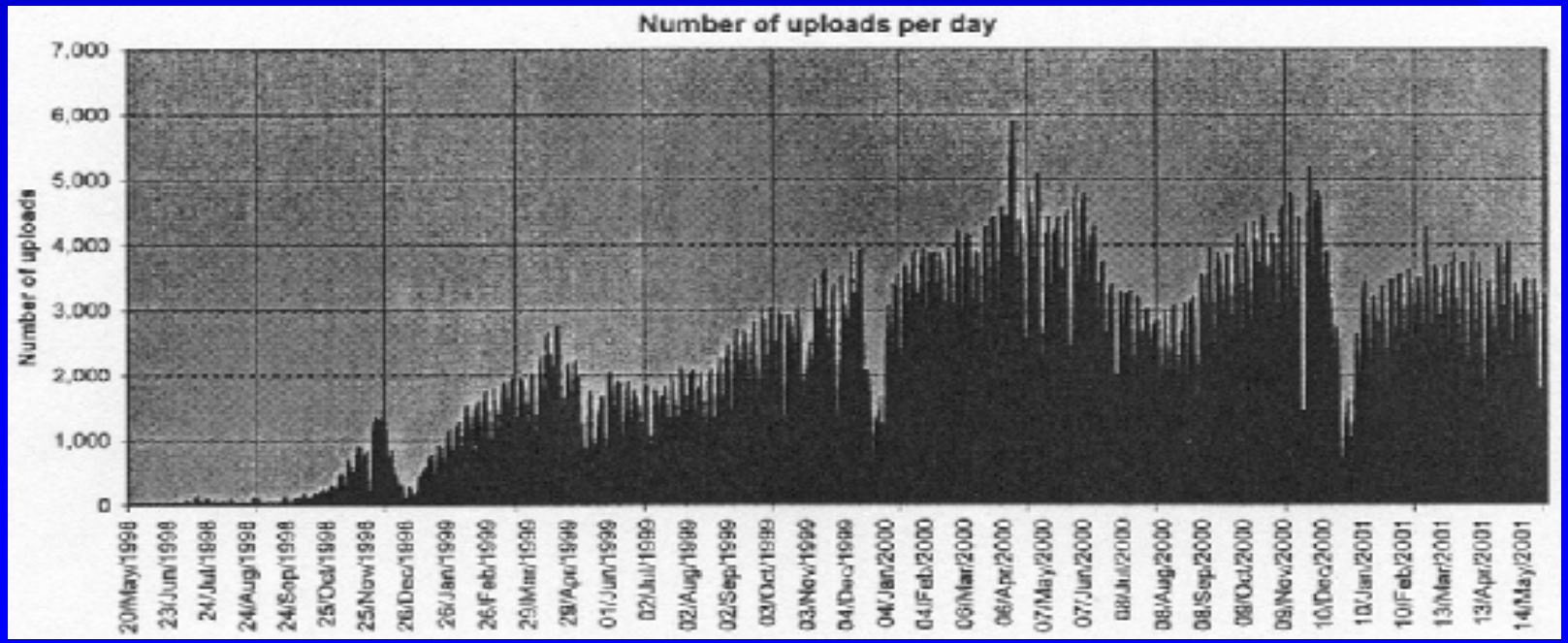


Virus samples

Why should we use old viruses ?

VESZPROG

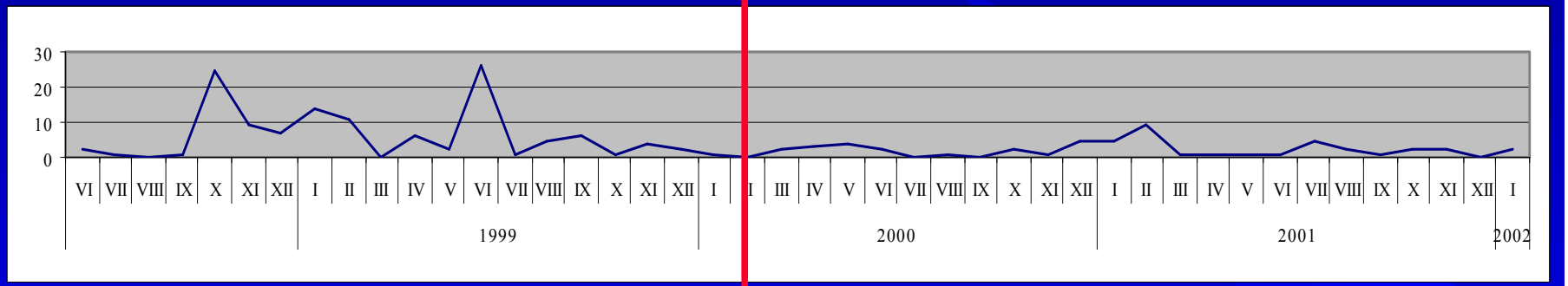


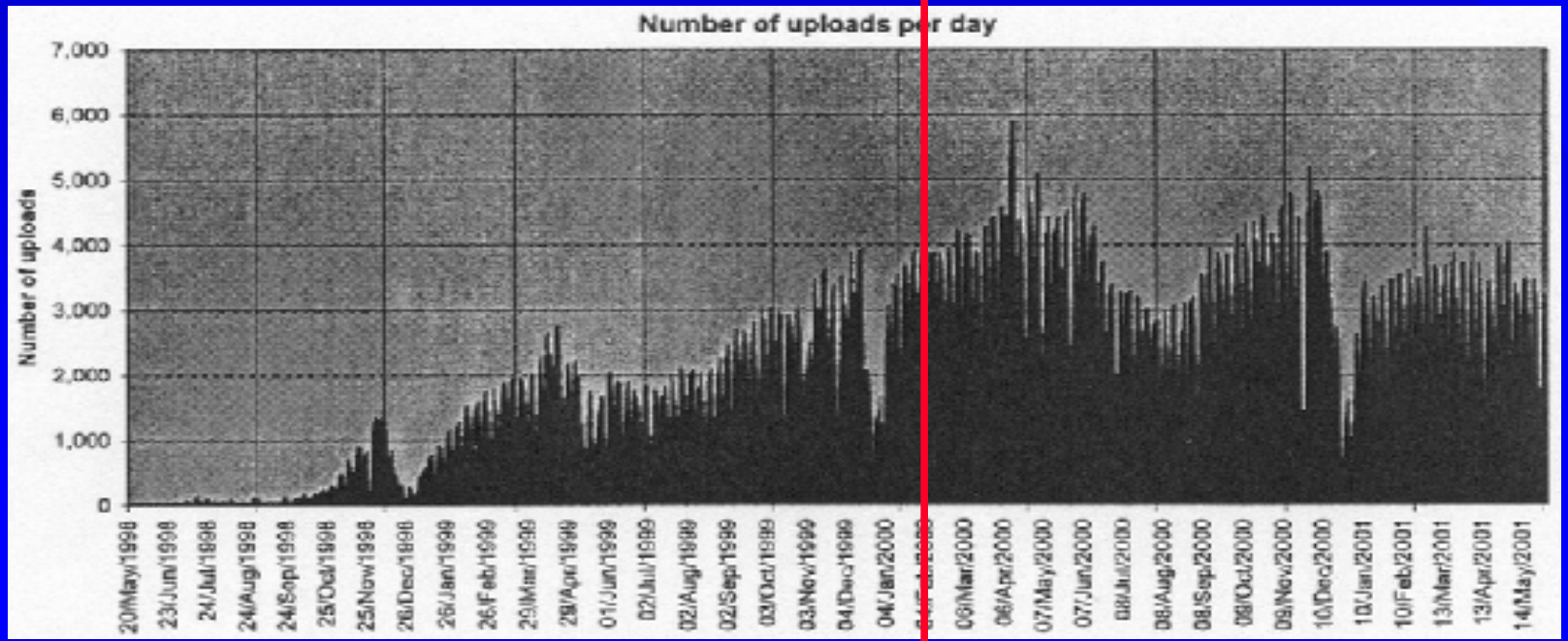


Virus samples

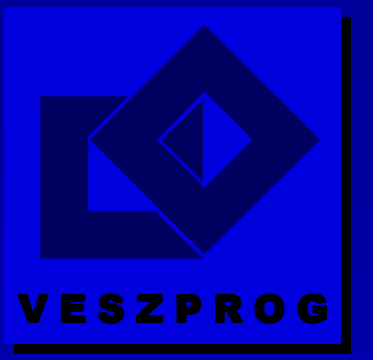
Why should we use old viruses ?

VESZPROG





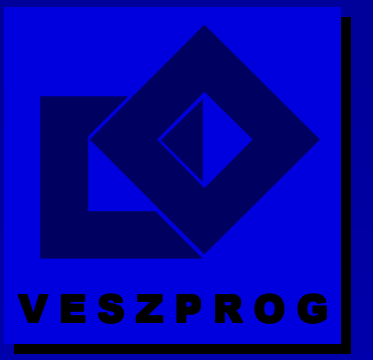
Virus samples



- Big number of samples should be replicated
- Test sets
  - ItW test set including old and new viruses
  - test set for testing the engine capability
- Which samples should be used ?
  - only virus samples (can infect other goats) or
  - samples modified by viruses (workable infection, bad infection, corrupted)

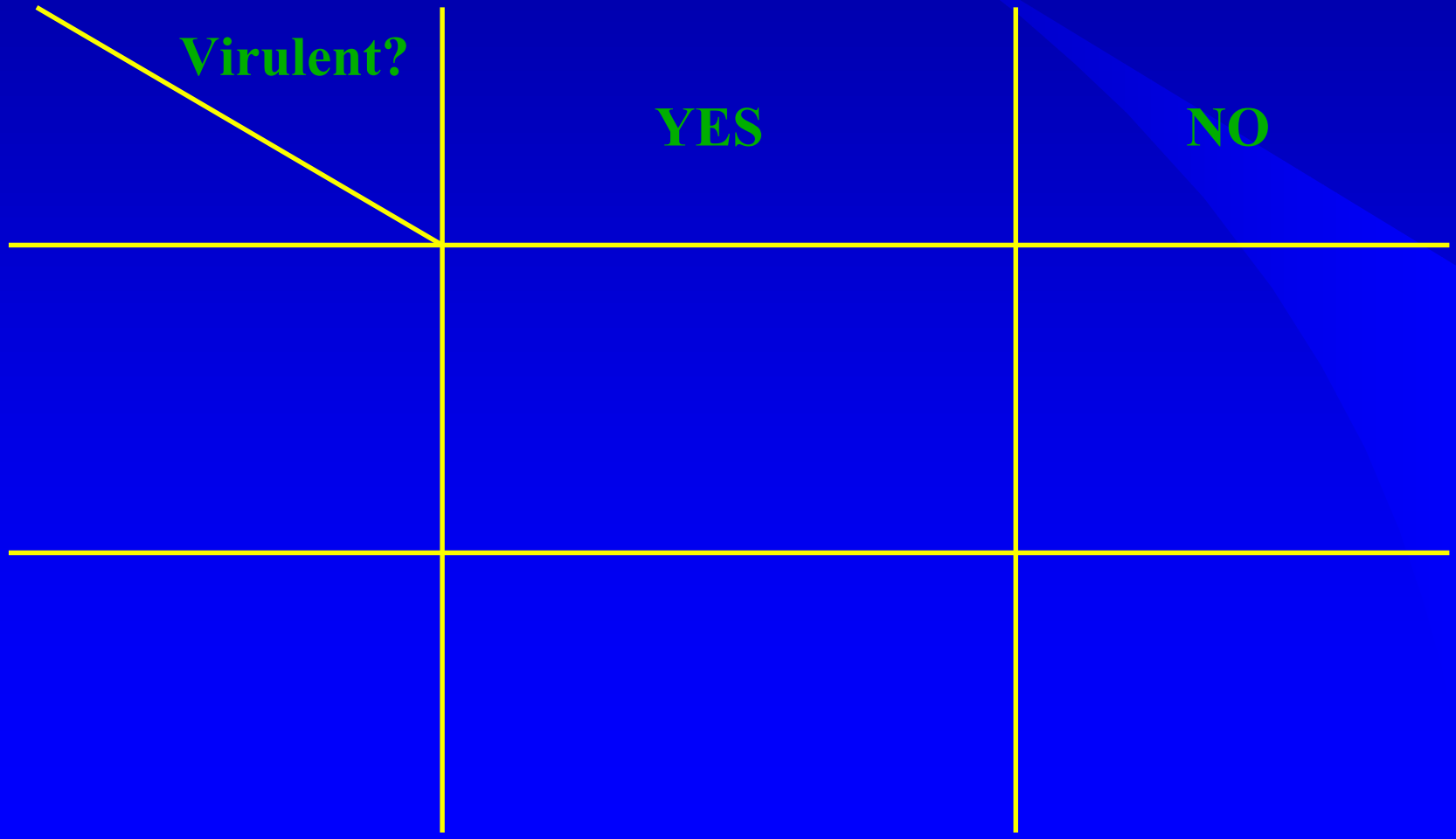
Virus samples

Which samples should be used ?



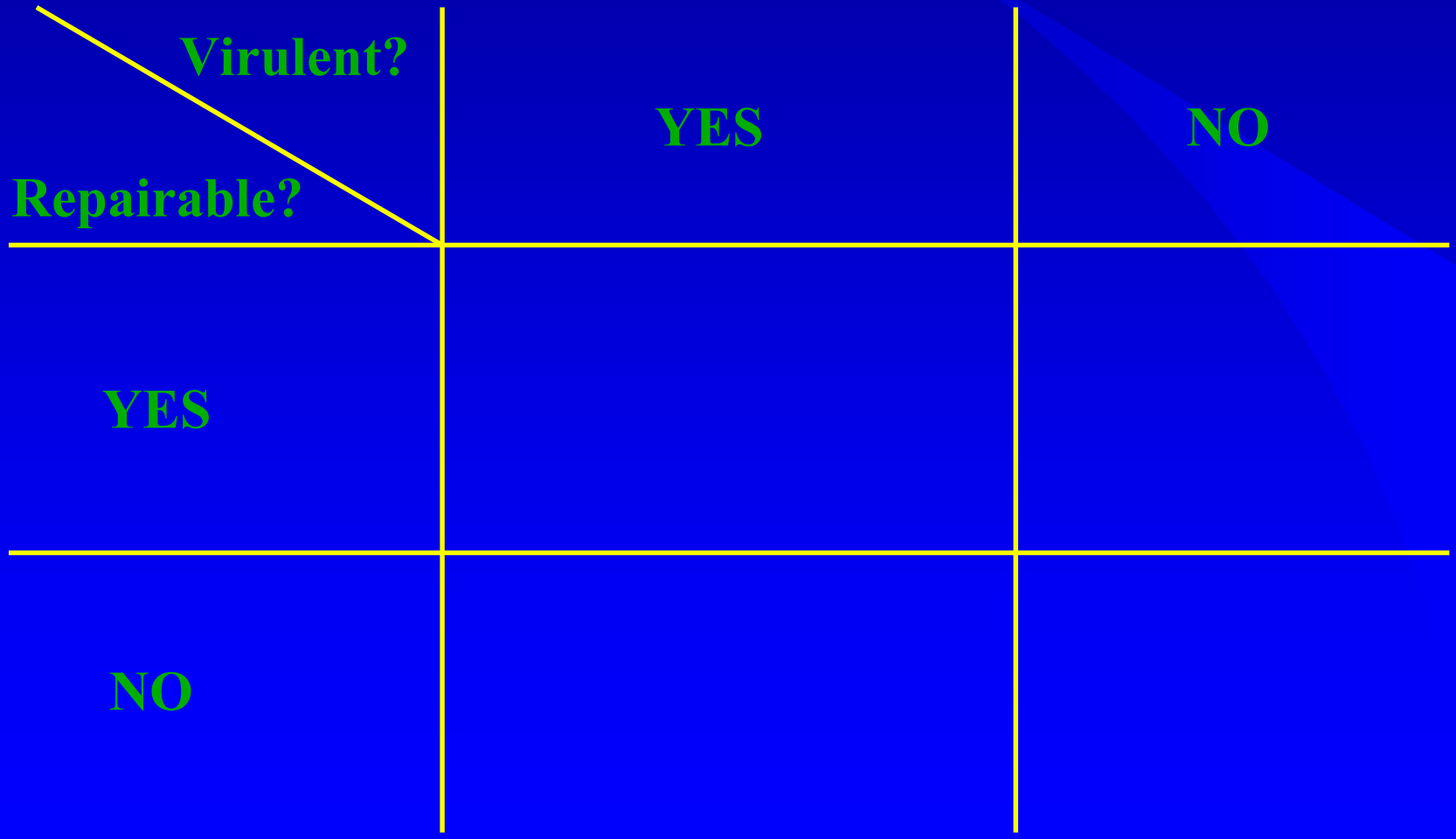
Virus samples

Which samples should be used ?



Virus samples

Which samples should be used ?

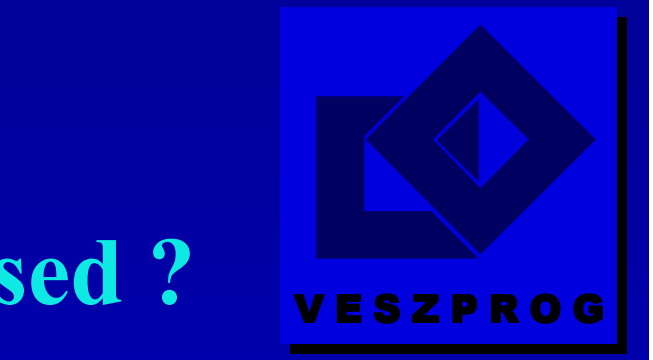


Virus samples

Which samples should be used ?

Virus samples

Which samples should be used ?



Virulent? / Repairable?	YES	NO
YES	(non-overwrite viruses) should be detected should be repaired	
NO	(overwrite viruses) should be detected	

Virus samples

Which samples should be used ?

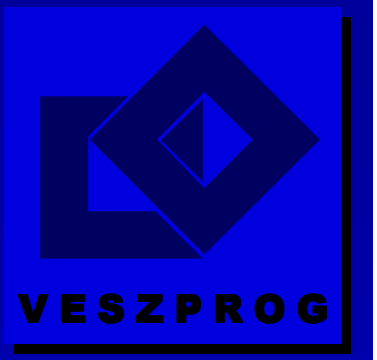
Virulent? / Repairable?	YES	NO
YES	(non-overwrite viruses) should be detected should be repaired	(wrong infections) should be detected should be repaired
NO	(overwrite viruses) should be detected	

Virus samples

Which samples should be used ?

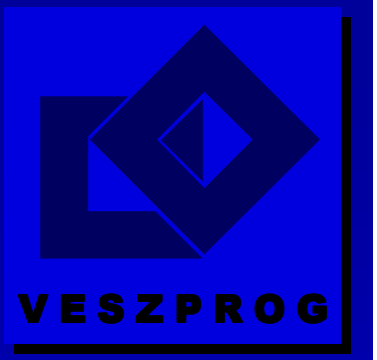
Virulent? / Repairable?	YES	NO
YES	(non-overwrite viruses) should be detected should be repaired	(wrong infections) should be detected should be repaired
NO	(overwrite viruses) should be detected	(corrupted items) should be detected

Executing AV product



- Different settings
  - on-access or on-demand scan
  - scan only or scan & kill
  - different options
- Execute in one step or separate the test collection
- Execute in real or in emulated environment

Analysing results (scanning test)



- AV should detect all of virus samples (if not -> PROBLEM)
- AV should identify the same virus in all of virus samples replicated from the same virus (if not -> BUG)
- Results of “different usages” of an AV product should be the same (if not -> BUG)

Analysing results (disinfection test)

VESZPROG

Disinfected samples

Analysing results (disinfection test)

VESZPROG

Infected samples

Disinfected samples

Really disinfected samples

Analysing results (disinfection test)

VESZPROG

Infected samples

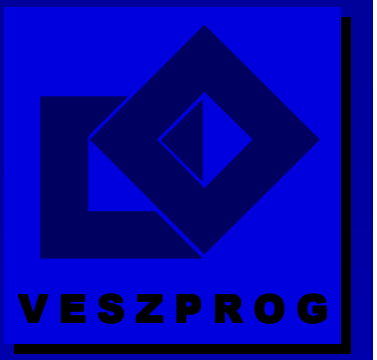
Disinfected samples

Really disinfected samples

Original goats

Intelligent compare

Analysing results (disinfection test)



Infected samples

Disinfected samples

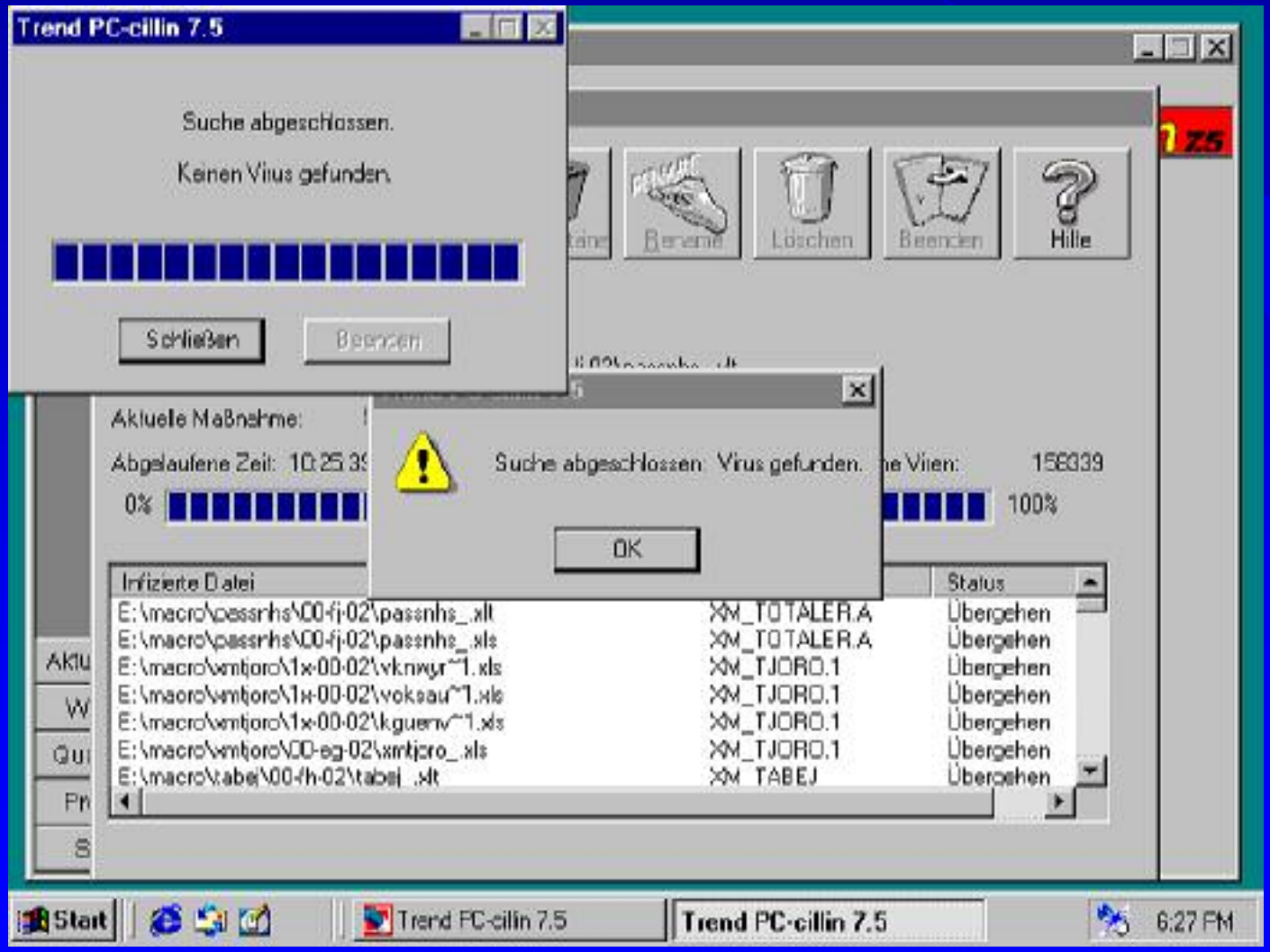
Really disinfected samples

Original goats

Intelligent compare

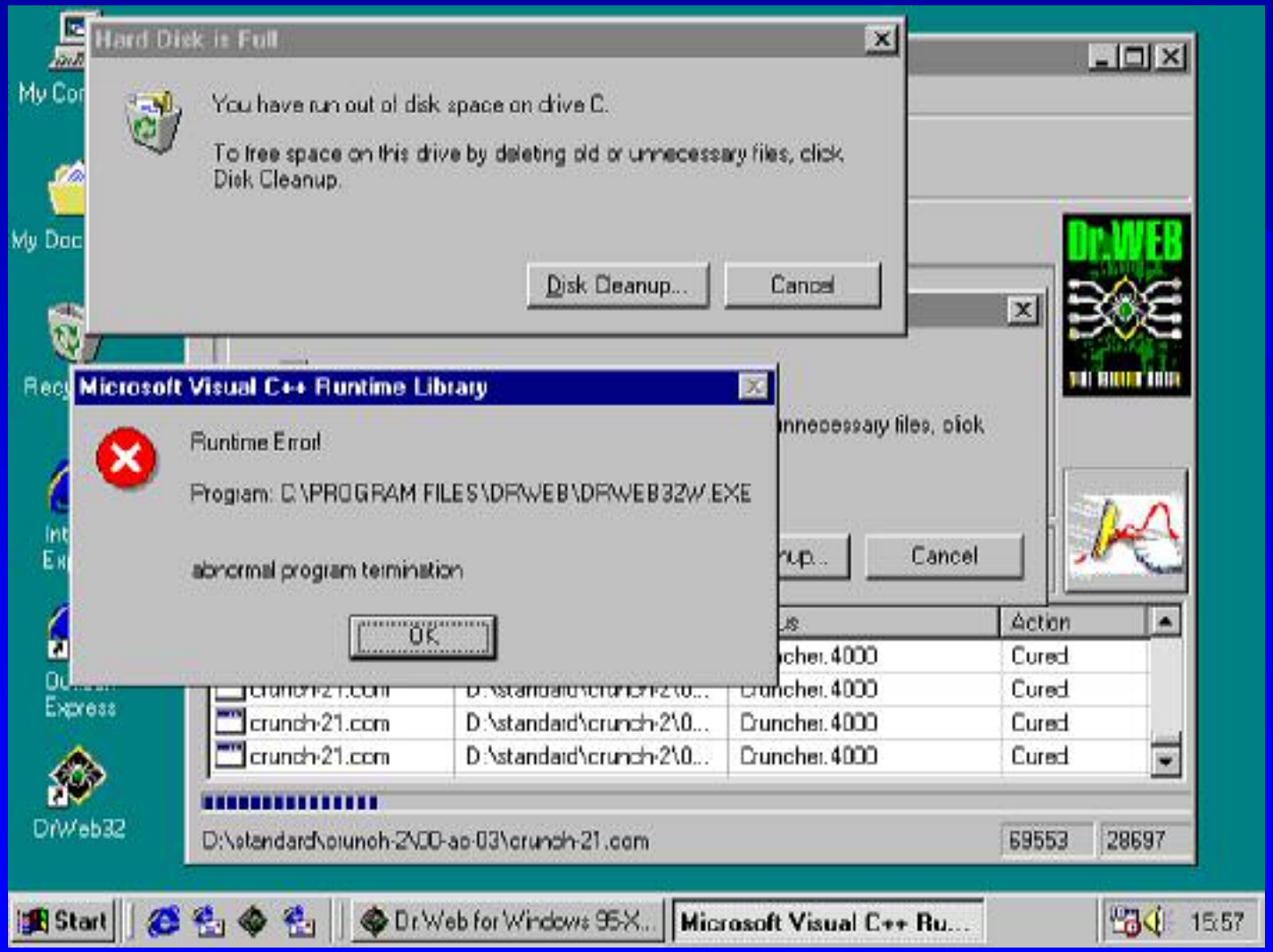
Results (flags)

Some interesting results



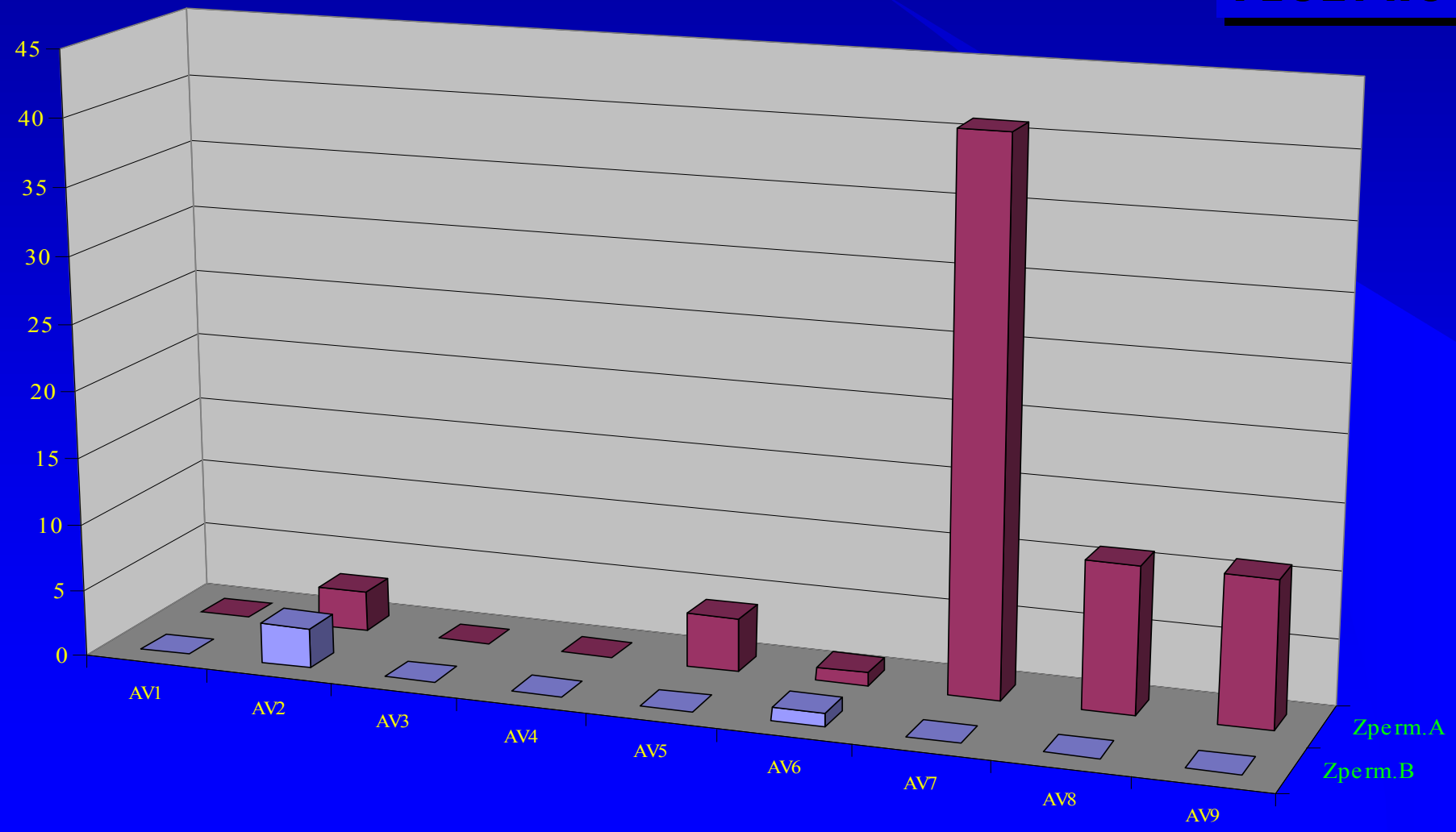
Some interesting results

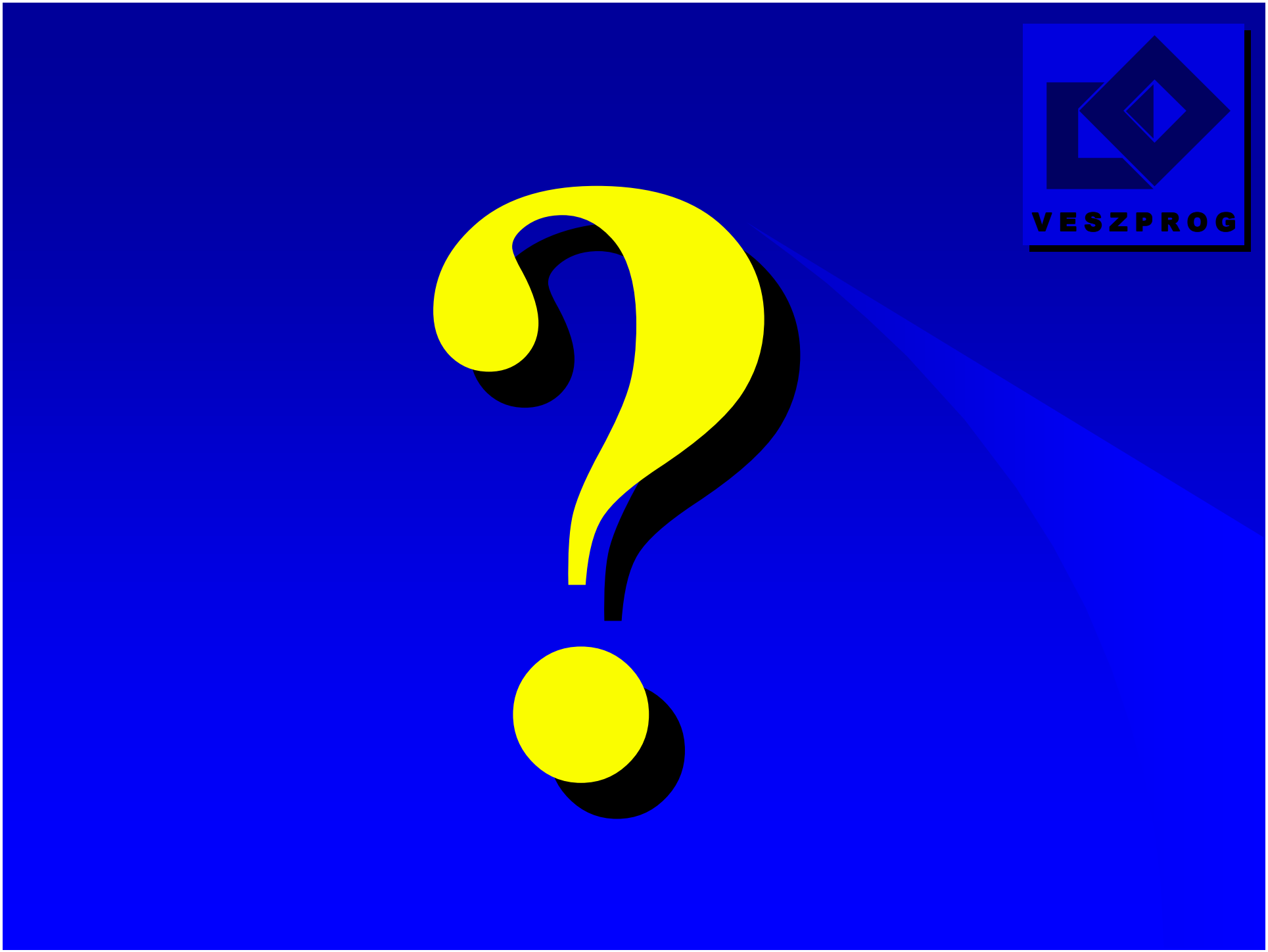
VESZPROG



An interesting result

VESZPROG




VESZPROG