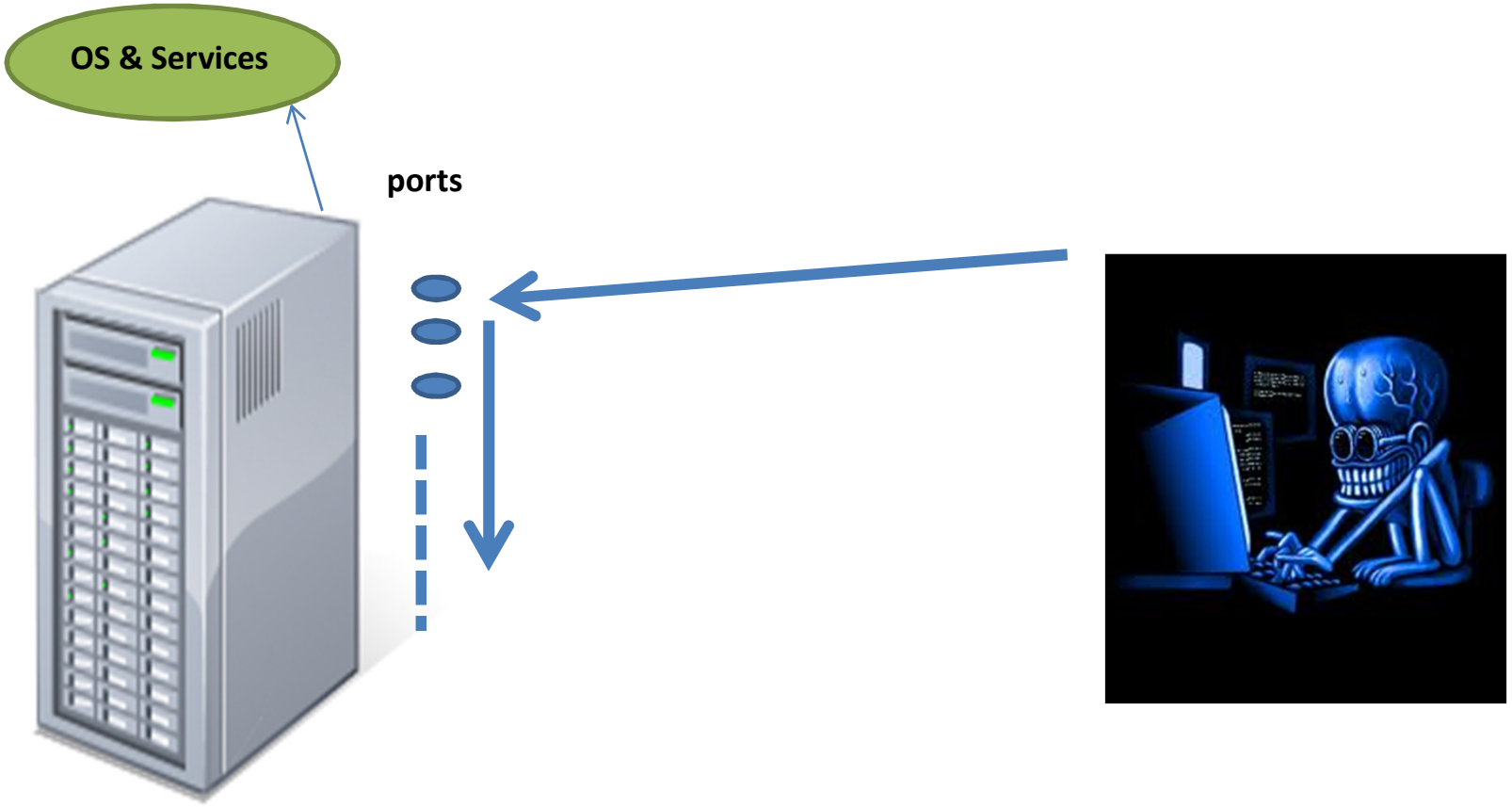
Application-Level Reconnaissance: Timing Channel Attacks Against Antivirus Software

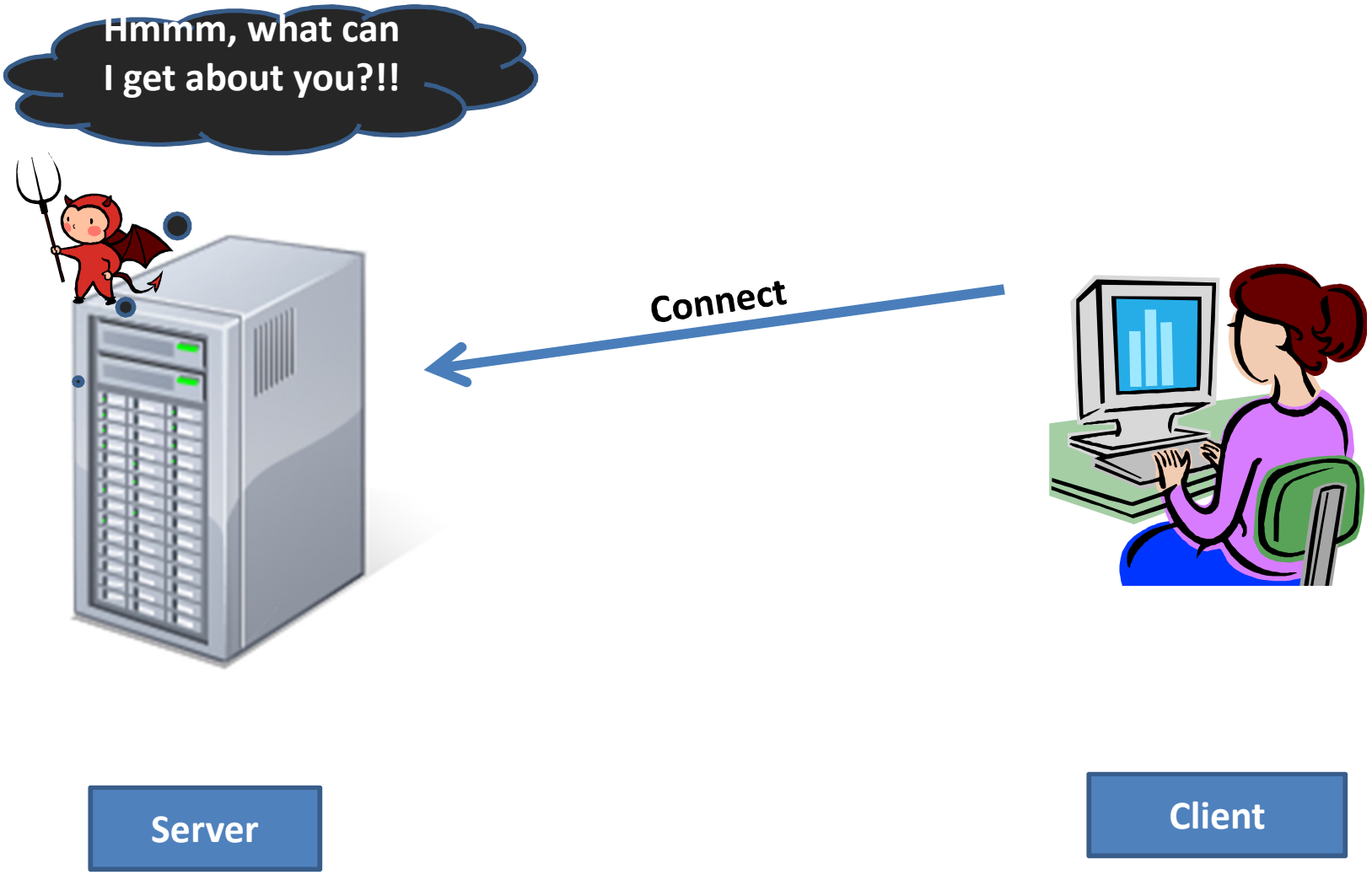
Mohammed I. Al-Saleh and Jedidiah R. Crandall

THE UNIVERSITY of NEW MEXICO

Server Reconnaissance



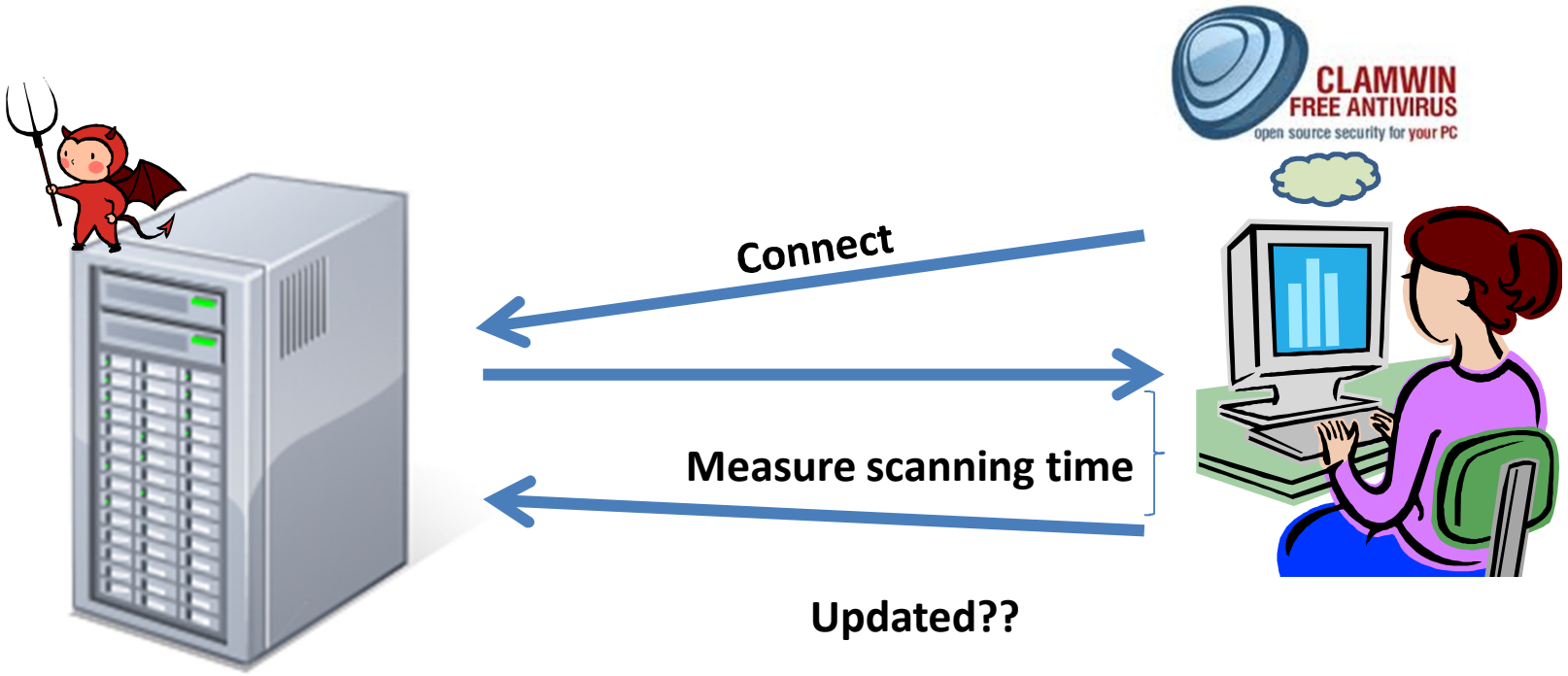
Client Reconnaissance



Client Reconnaissance

- Browser identification
  - https://panopticlick.eff.org/
- AV related info
  - AV fingerprinting
  - Up-to-date?
- Timing channels
  - AV performance tradeoff
  - Make the common case fast
  - Updated?

Threat Model



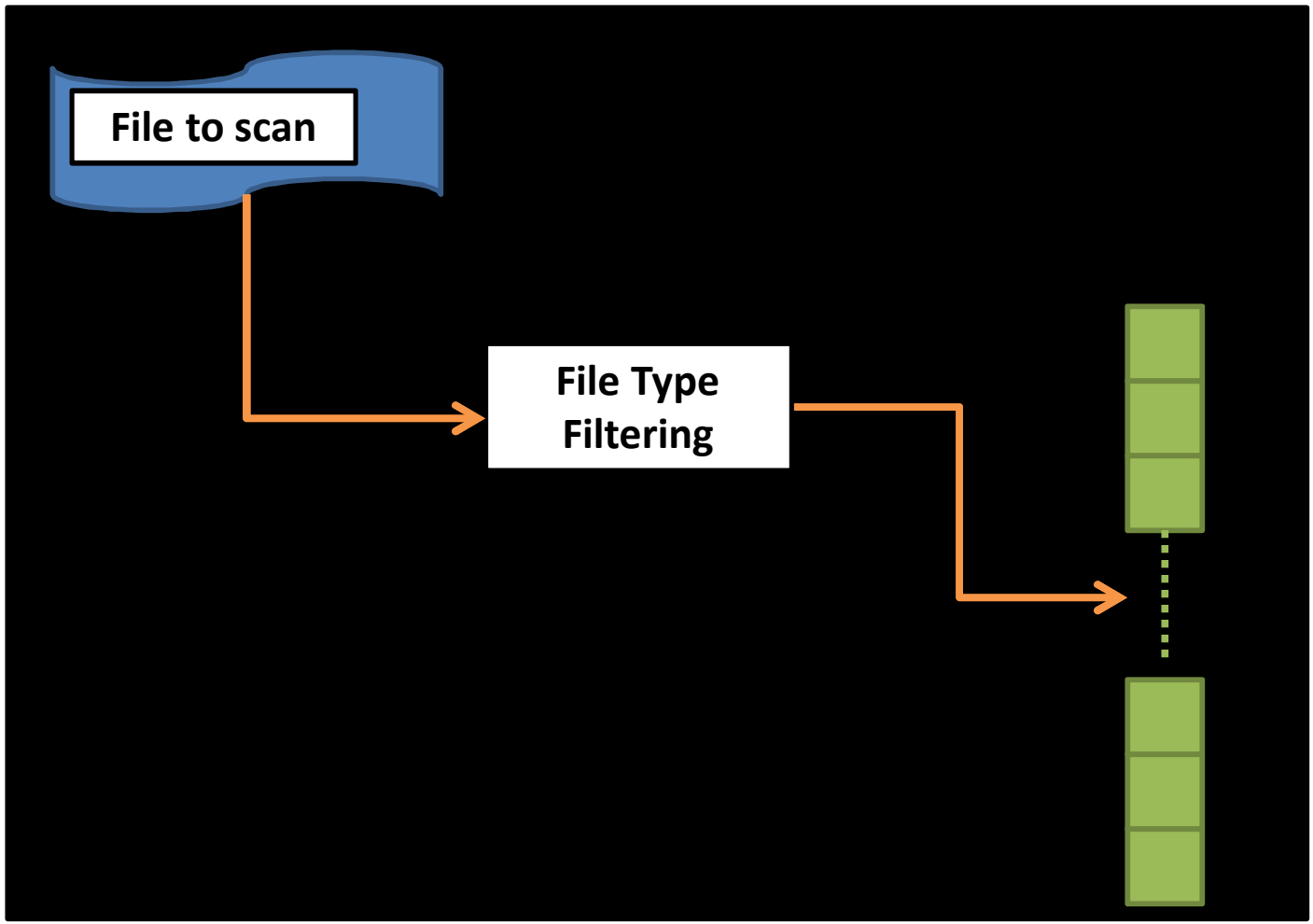
Basic Idea

- Antivirus (AV) scans data against sigs
- Sigs are stored somehow in AV's data structures
- Scanning time
  - Based on scanning path
- Hitting the newly added sigs

ClamAV

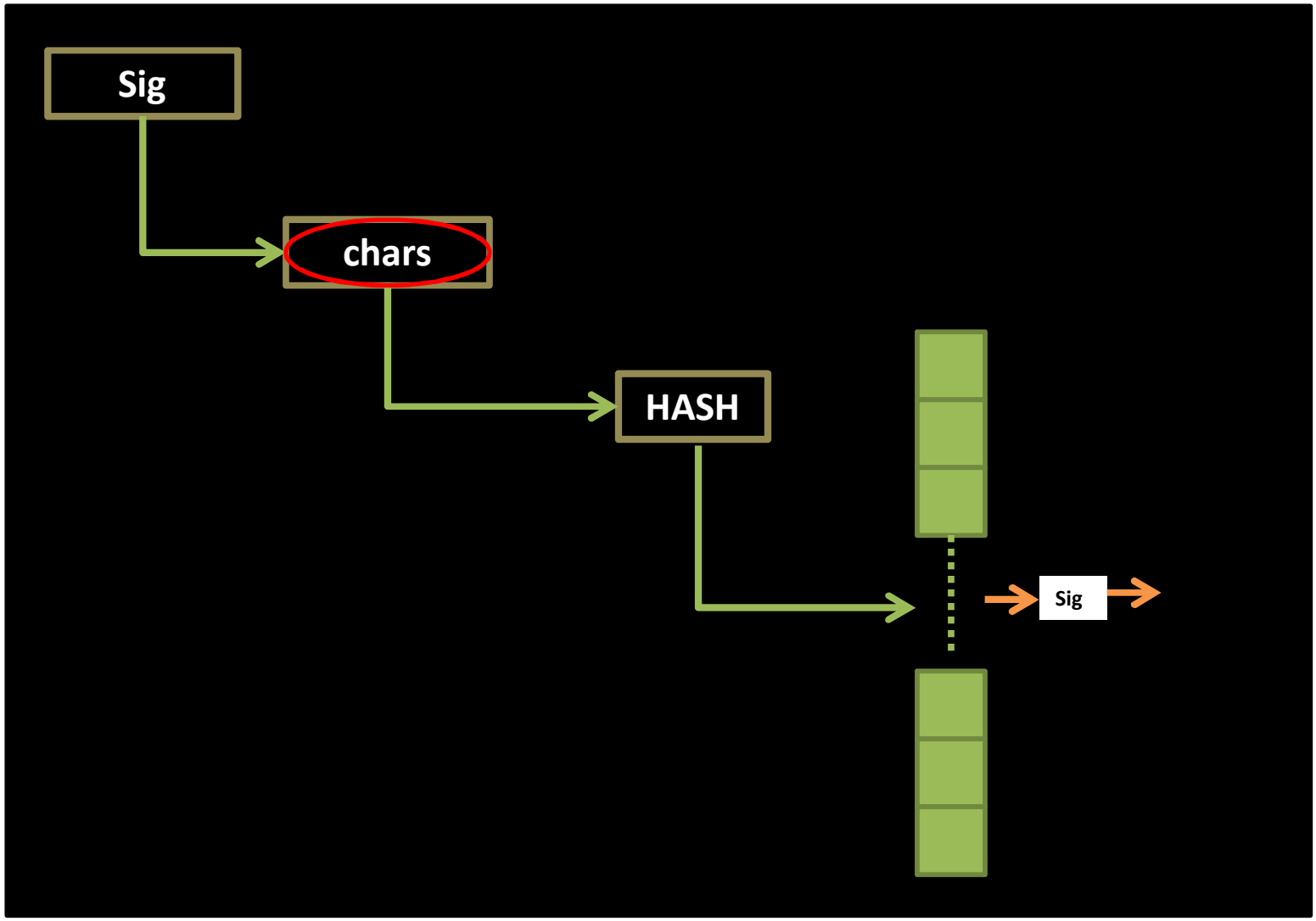
- ClamAV
  - http://www.clamav.net
  - http://www.clamxav.com/
  - http://www.clamwin.com/
- Scanning steps:
  - File type filtering
  - Filtering step
  - Boyer-Moore algorithm
  - Aho-Corasick algorithm

File Type Filtering

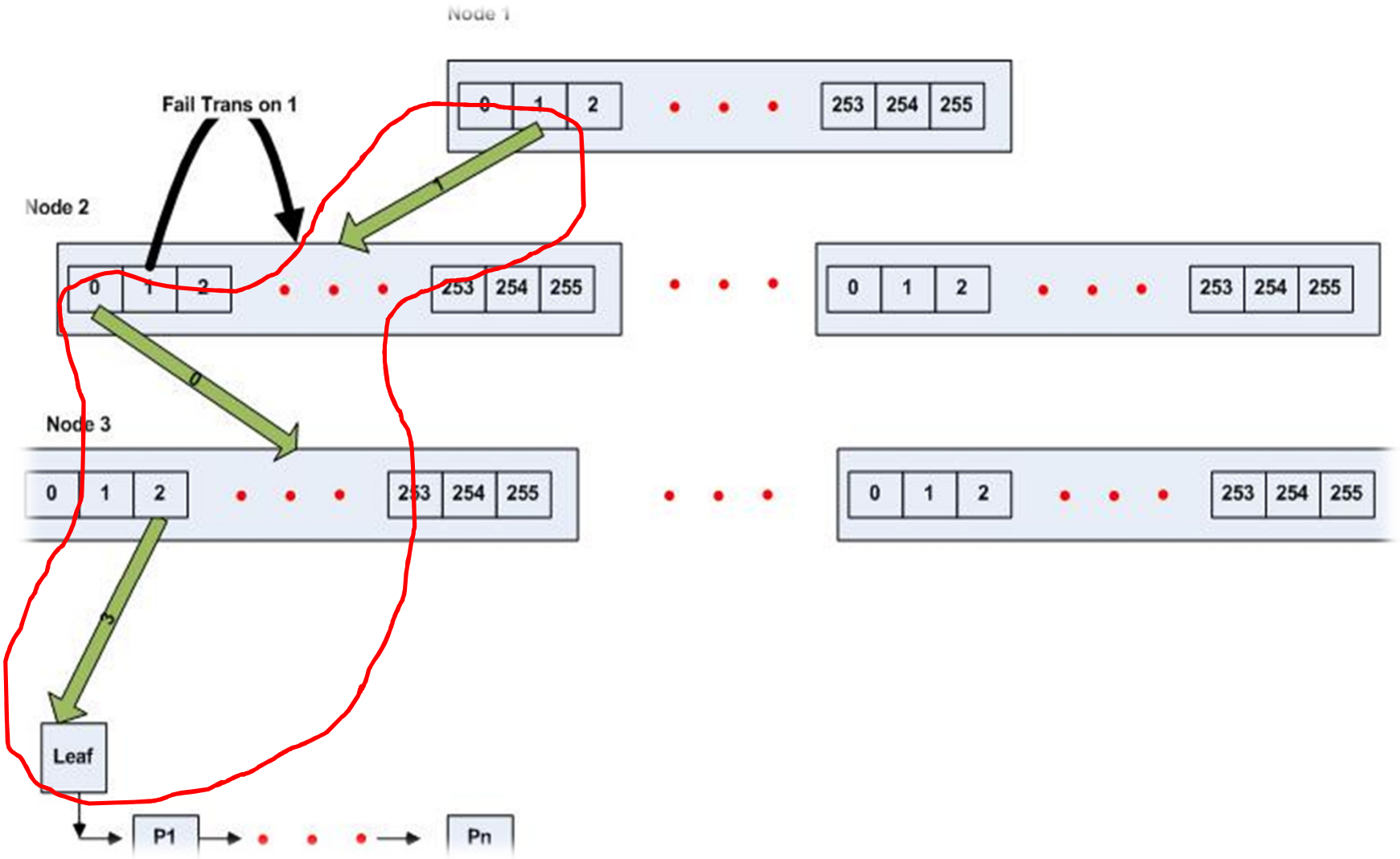


Filtering Step

Boyer-Moore



Aho-Corasick



Methodology

- **Question #1**: Is there a timing channel in the way ClamAV scans data?

- **Question #2**: If the first question is confirmed, how could the attacker create the timing channel?

Methodology/Q1

- Collect viruses in (name,date) pairs and remove their sigs from current DB

Author: Robert Scroggins
Date: 2011-01-14 18:23 -700
To: clamav-virusdb
Subject: [clamav-virusdb] Update (daily: 12521)

ClamAV database updated (14 Jan 2011 20-22 -0500): daily.cvd
Version: 12521

Submission-ID: 20778735
Sender: Virus Total
Sender: Anonymous
Added: Trojan.Ransom-649
Virus name alias: Trojan-Ransom.MSIL.FakeInstaller.d (Kaspersky)

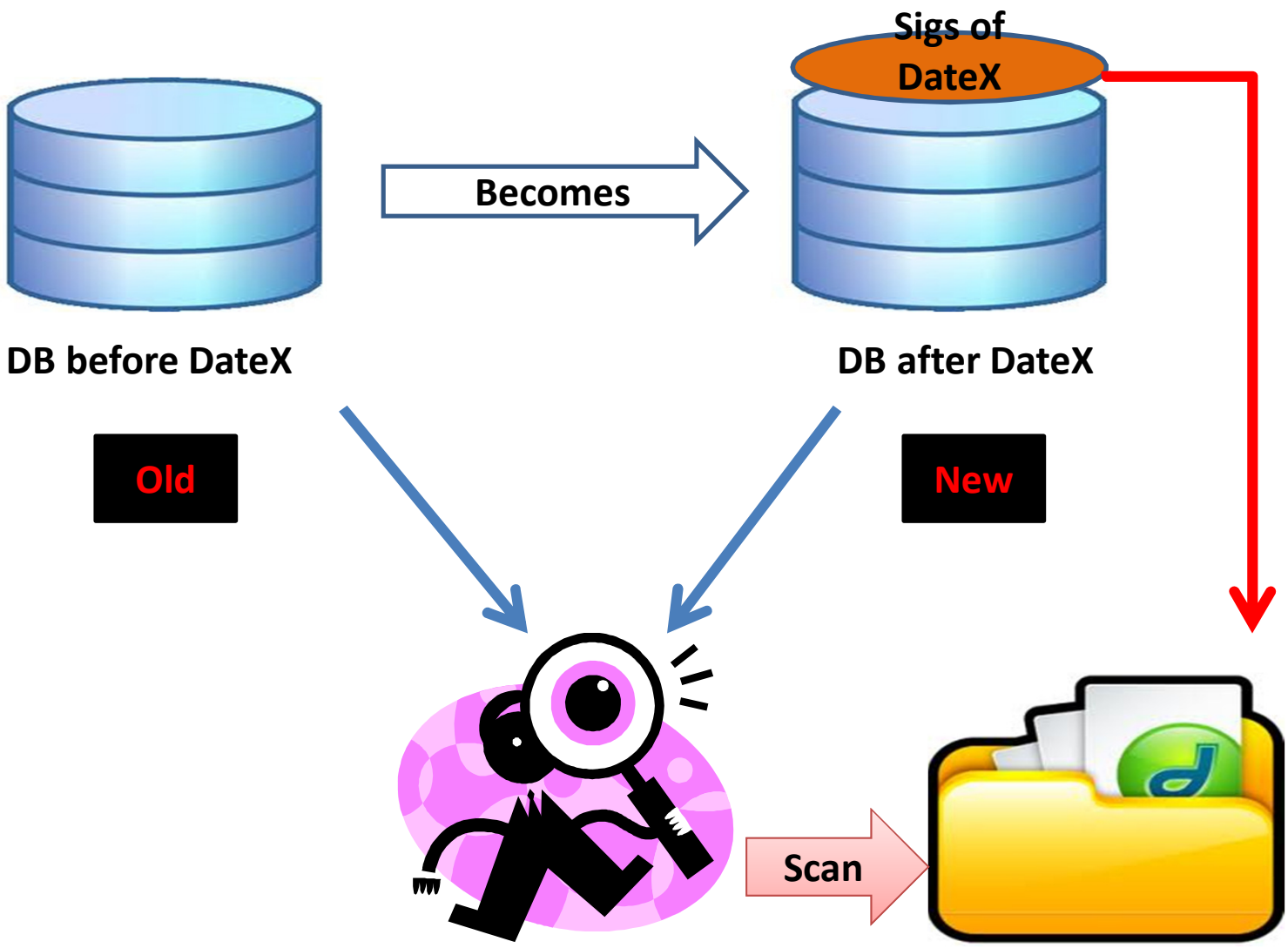
Submission-ID: 20372740
Sender: Dave M
Sender: Jotti
Sender: Virus Total
Added: Backdoor.Agent-40
Virus name alias: Backdoor.Win32.Agent.bdnl (Kaspersky)

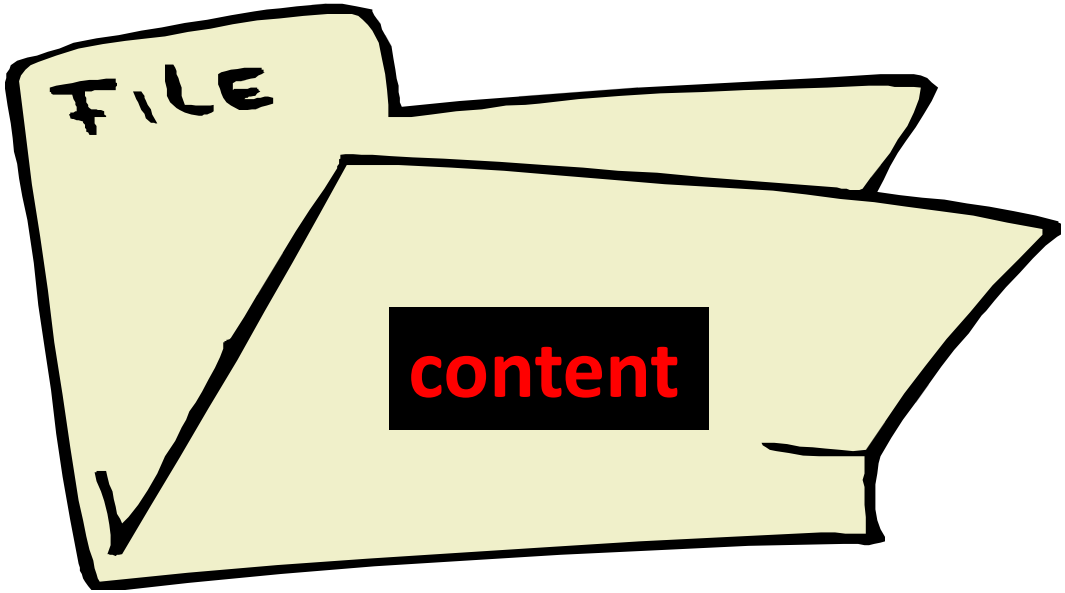
▪▪▪▪▪▪▪▪

Two Kinds of Experiments

- Whole-day sig experiment
- Single sig experiment

Whole-Day


Sigs of DateX
Becomes
DB before DateX
DB after DateX
Old
New
Scan

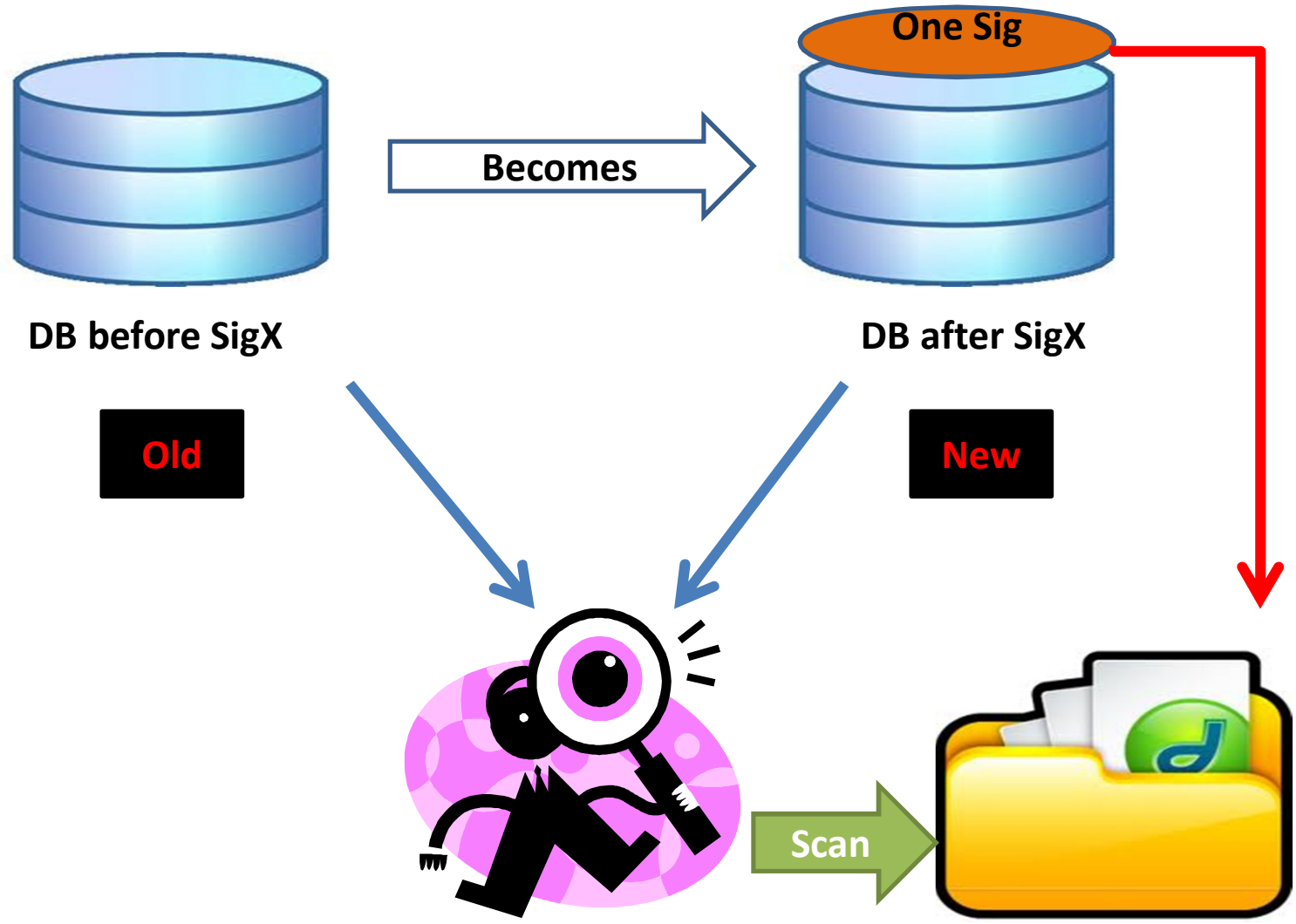


BuffSize = 256 KB

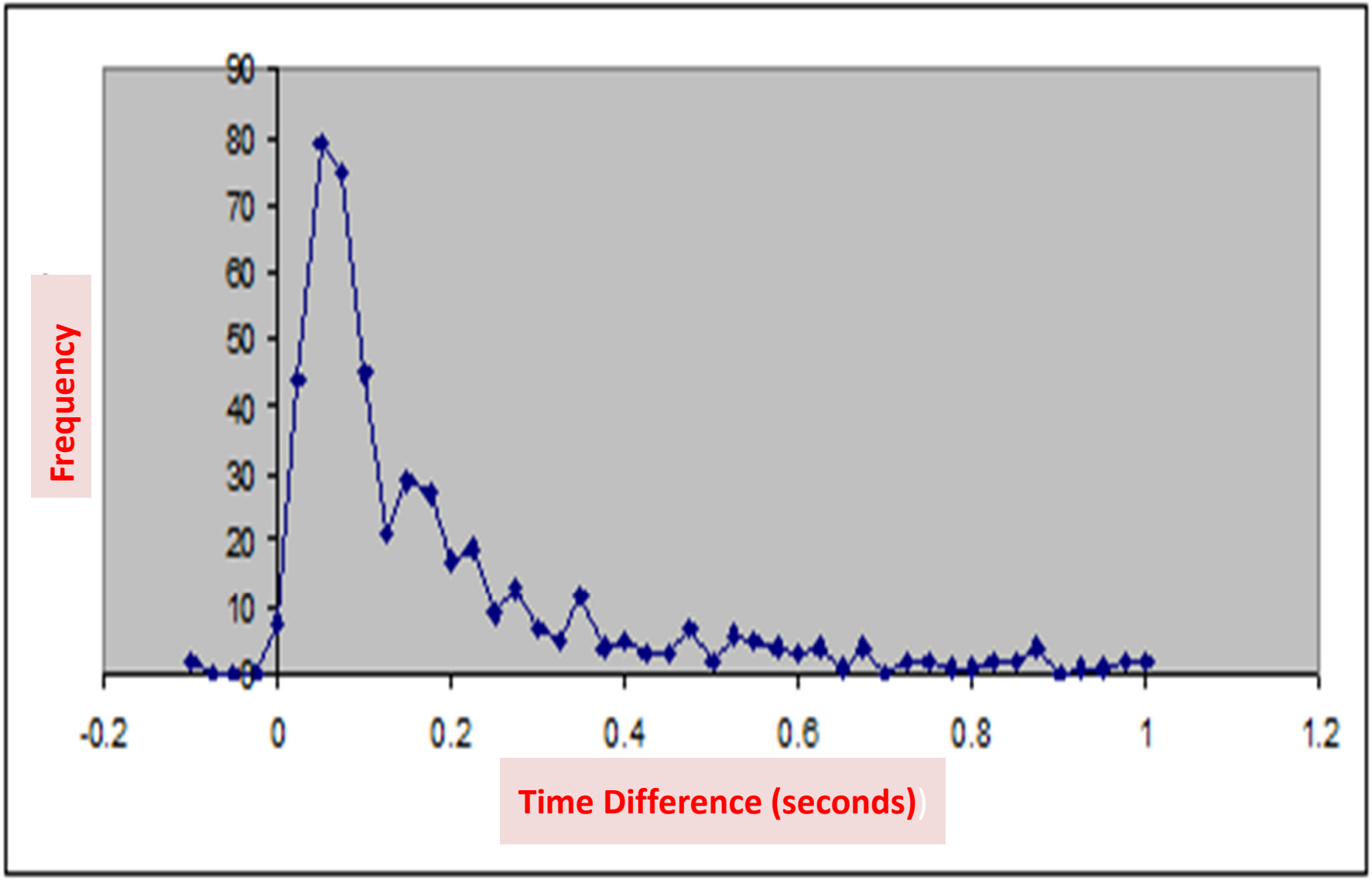
(((ahochars|boyerchars)^n . filterchars)^m)

File Size

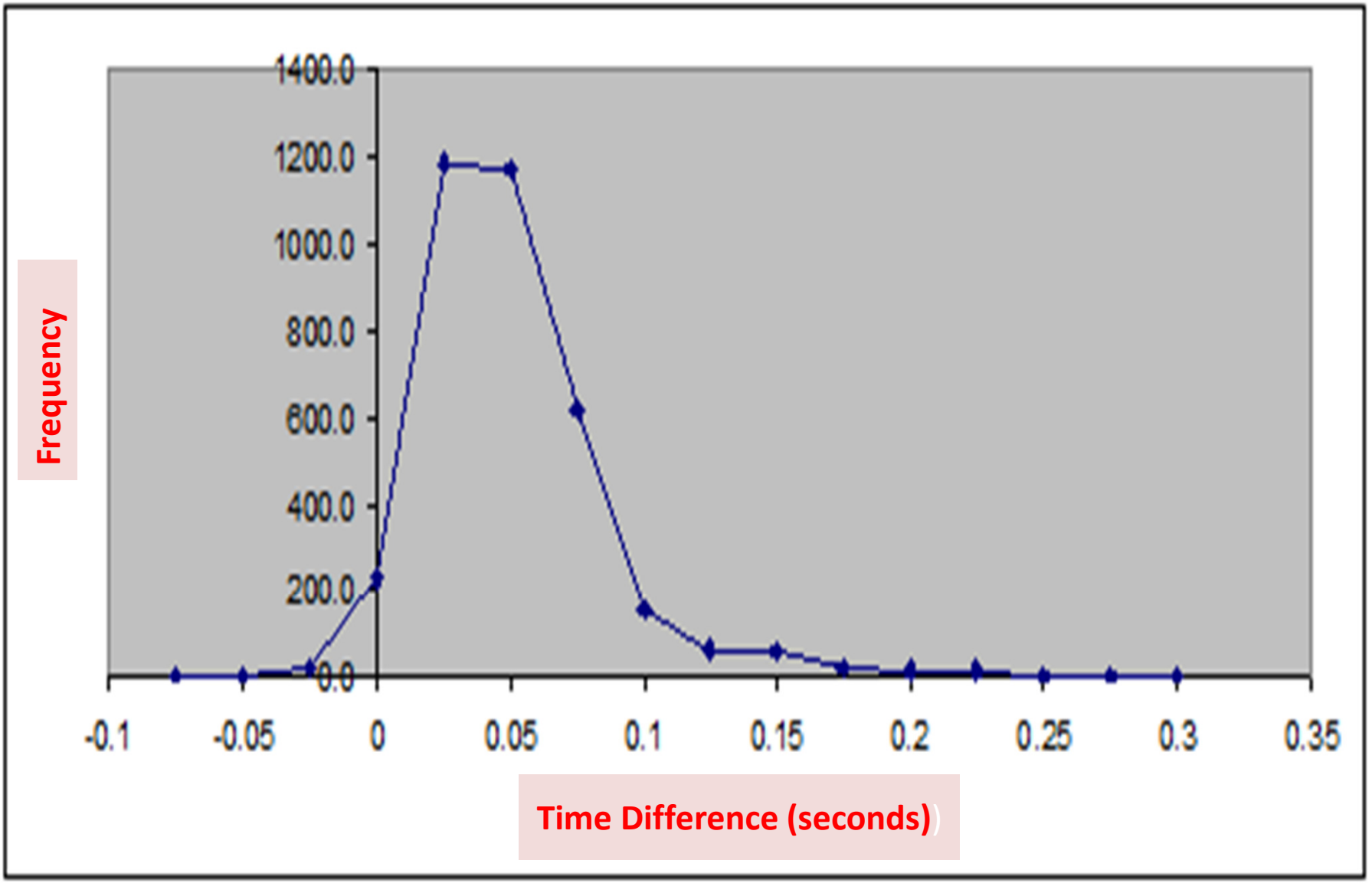
Single Signature



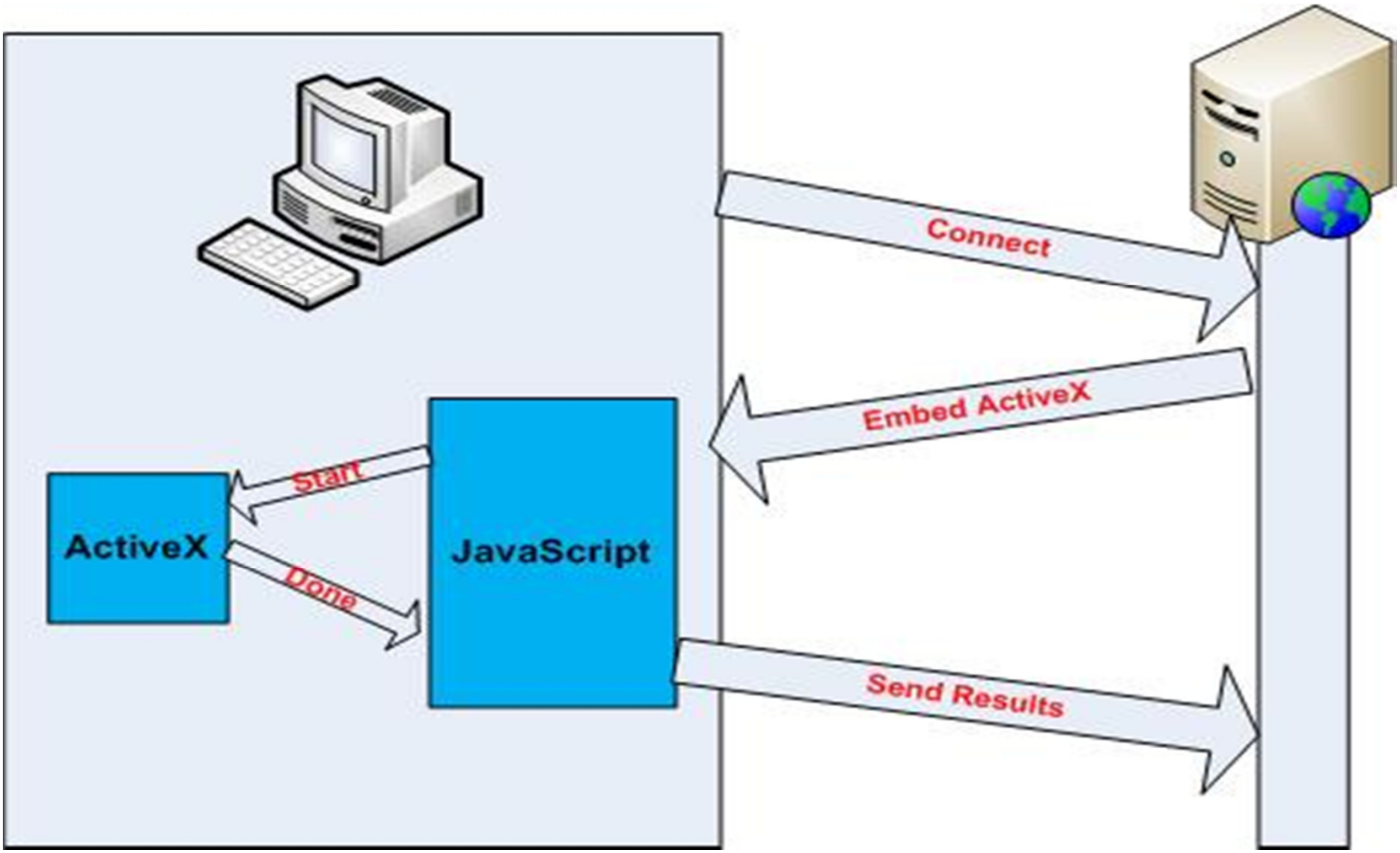
Whole-Day


Frequency
90
80
70
60
50
40
30
20
10
0
-0.2
0
0.2
0.4
0.6
0.8
1
1.2
Time Difference (seconds)

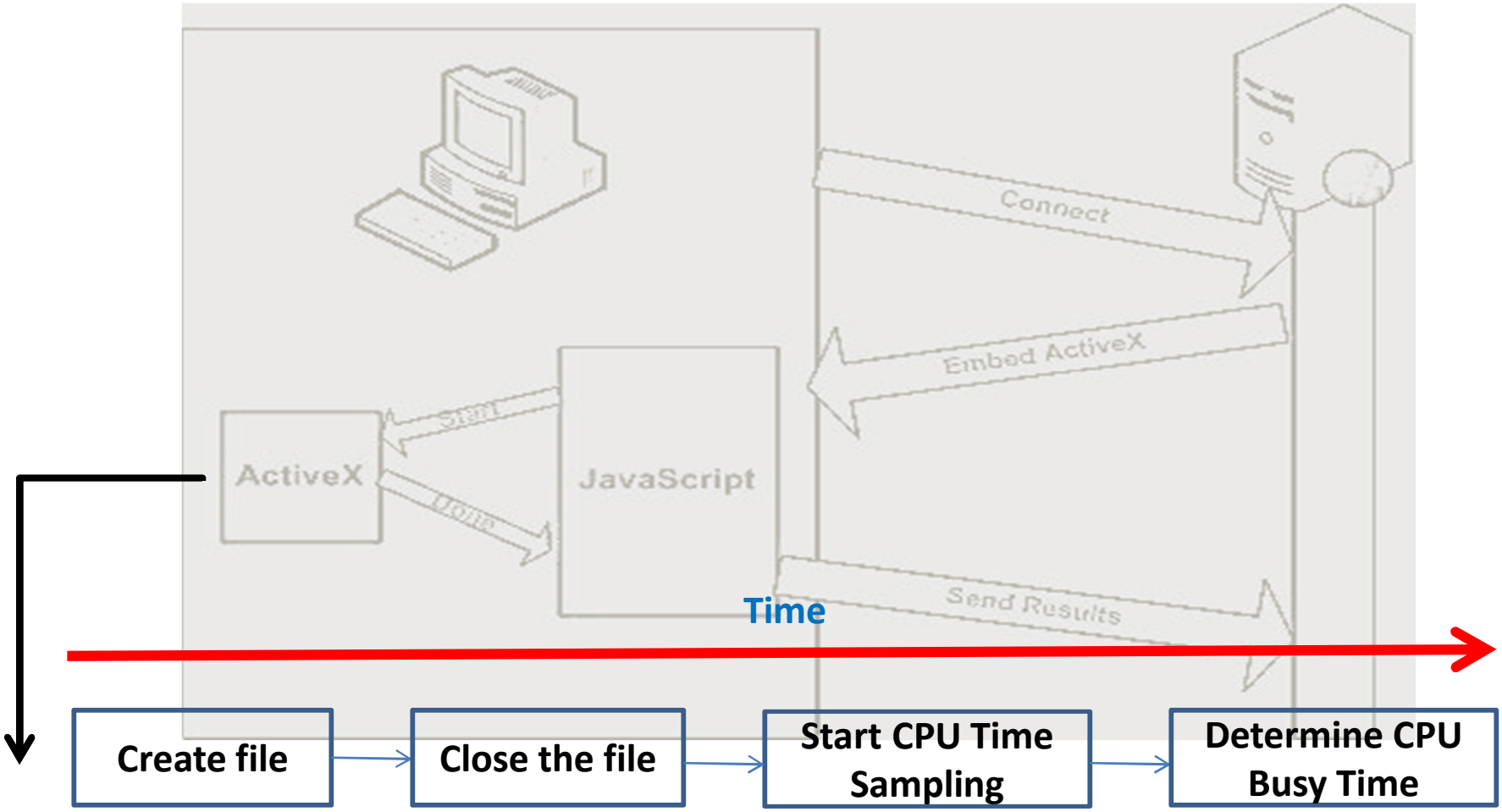
Single


Frequency
1400.0
1200.0
1000.0
800.0
600.0
400.0
200.0
0.0
-0.1
-0.05
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
Time Difference (seconds)

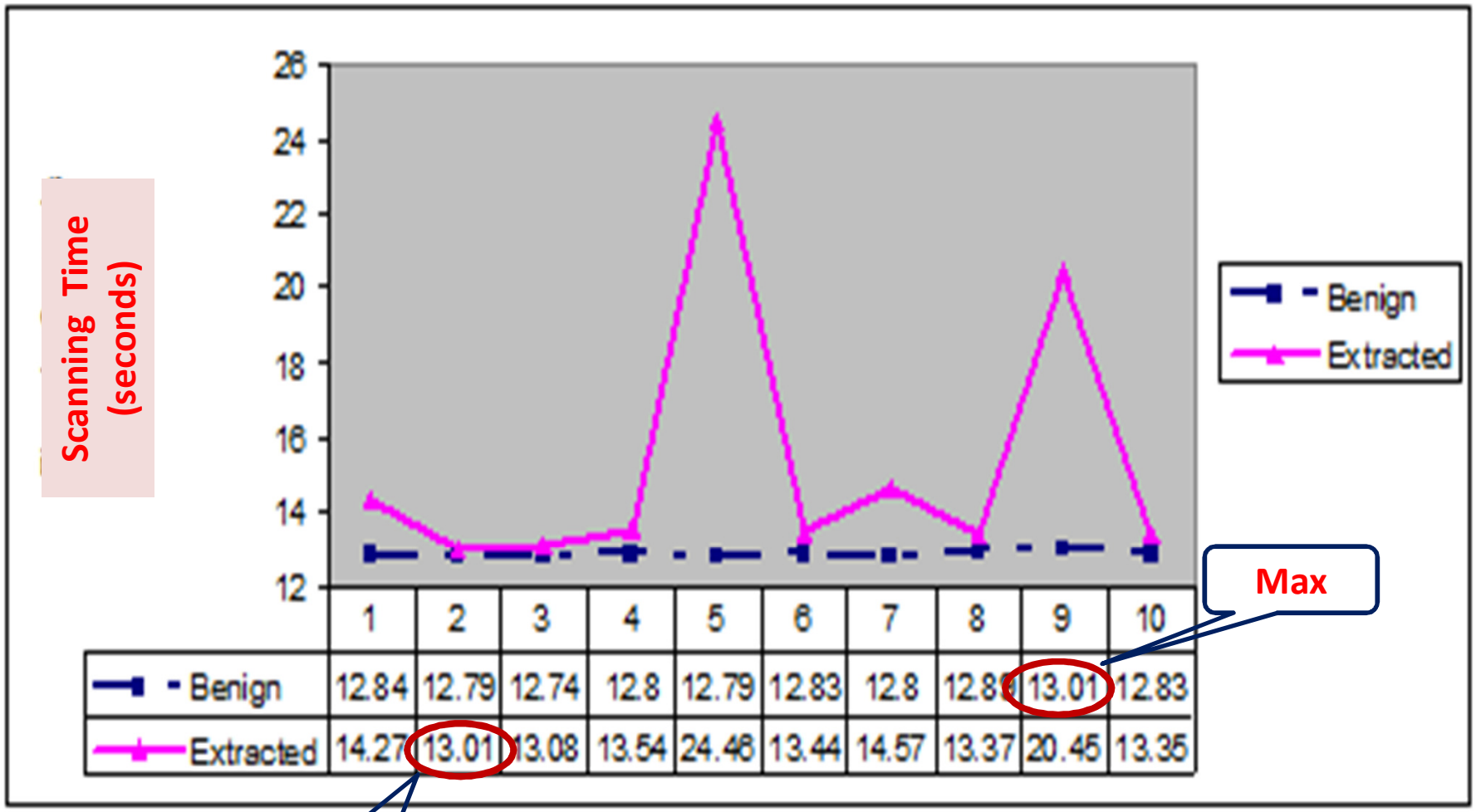
Methodology/Q2



Methodology/Q2



ActiveX



	1	2	3	4	5	6	7	8	9	10
Benign	12.84	12.79	12.74	12.8	12.79	12.83	12.8	12.8	13.01	12.83
Extracted	14.27	13.01	13.08	13.54	24.46	13.44	14.57	13.37	20.45	13.35

Possible Timing Channels in Modern AVs

- Pattern matching
- Algorithmic scanning
  - Zmist virus needs to execute at least 2 million p-code-based iterations
- Code emulation
  - Significantly slows scanning
- Heuristics
  - Extra work when triggered

Related Work

- Network discovery
  - Port scanning
- Timing channel attacks
  - Secret keys in cryptographic systems
  - Virtual machines detection
  - Others
- Antivirus research
  - Signature extraction
  - Detection evasion

Conclusion and Future Work

- Application-level reconnaissance through timing channels
- Running example: ClamAV
- Currently, we are exploring performance issues in commercial antiviruses

Acknowledgements

- Török Edwin
- LEET reviewers
- U.S. National Science Foundation (CNS-0905177)

Thanks