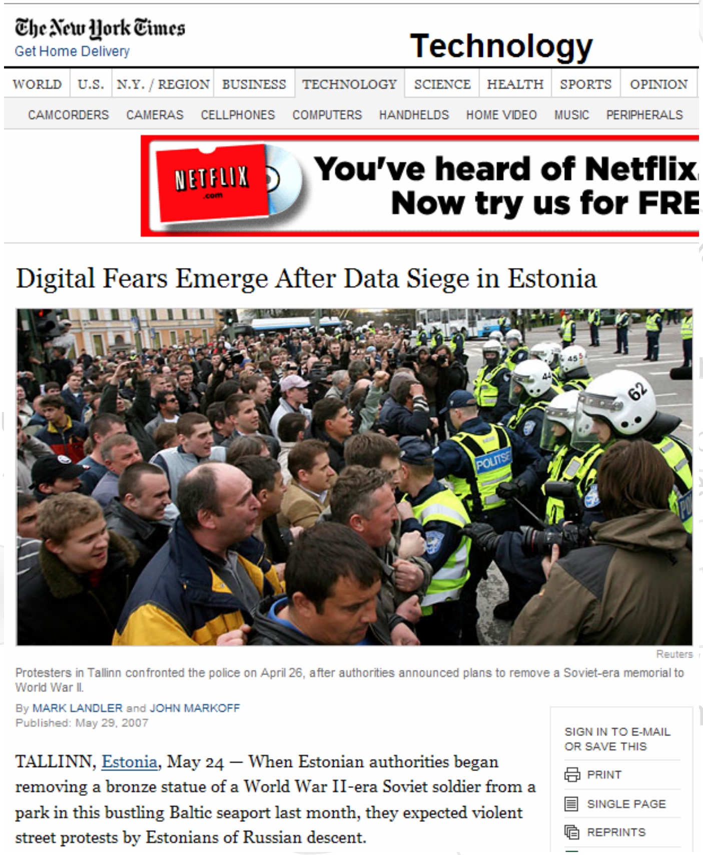
WetStone
A Division of Allen Corporation

Polymorphic & Metamorphic Malware

Chet Hosmer, Chief Scientist

Black Hat
BRIEFINGS AND TRAINING

Malware Impact



The New York Times
Get Home Delivery

Technology

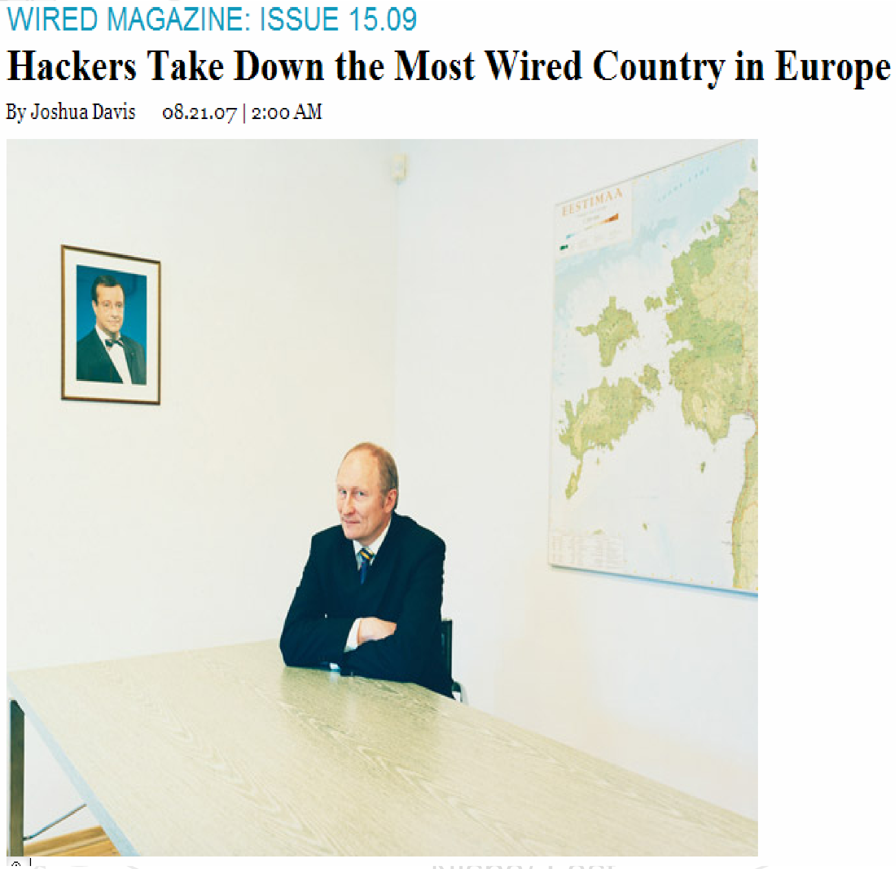
Digital Fears Emerge After Data Siege in Estonia

Reuters

Protesters in Tallinn confronted the police on April 26, after authorities announced plans to remove a Soviet-era memorial to World War II.

By MARK LANDLER and JOHN MARKOFF
Published: May 29, 2007

TALLINN, Estonia, May 24 — When Estonian authorities began removing a bronze statue of a World War II-era Soviet soldier from a park in this bustling Baltic seaport last month, they expected violent street protests by Estonians of Russian descent.



WIRED MAGAZINE: ISSUE 15.09

Hackers Take Down the Most Wired Country in Europe

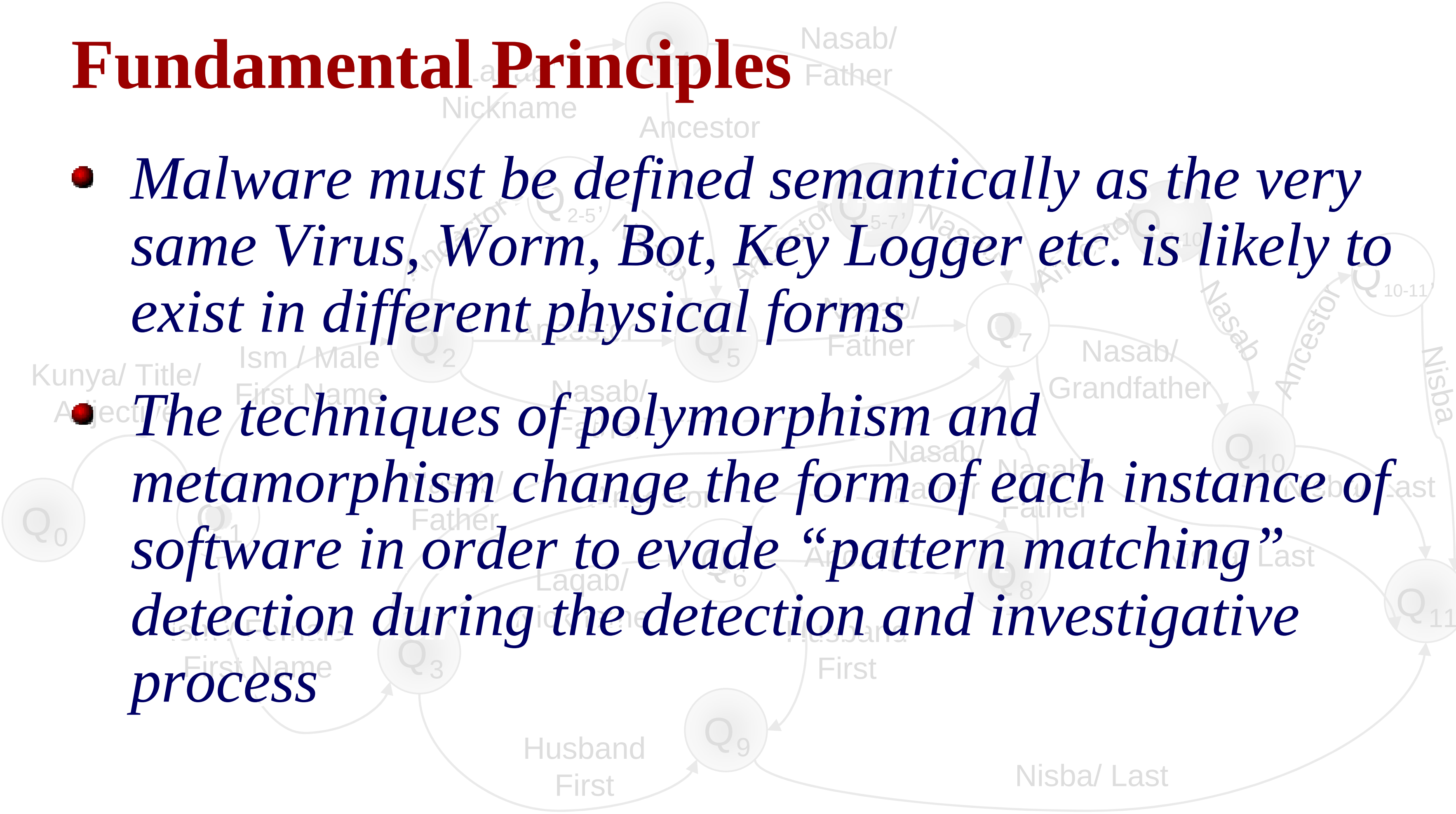
By Joshua Davis 08.21.07 | 2:00 AM

Source: NY Times and Washington Post

Metamorphic / Polymorphic Malware

Fundamental Principles

- *Malware must be defined semantically as the very same Virus, Worm, Bot, Key Logger etc. is likely to exist in different physical forms*
- *The techniques of polymorphism and metamorphism change the form of each instance of software in order to evade "pattern matching" detection during the detection and investigative process*

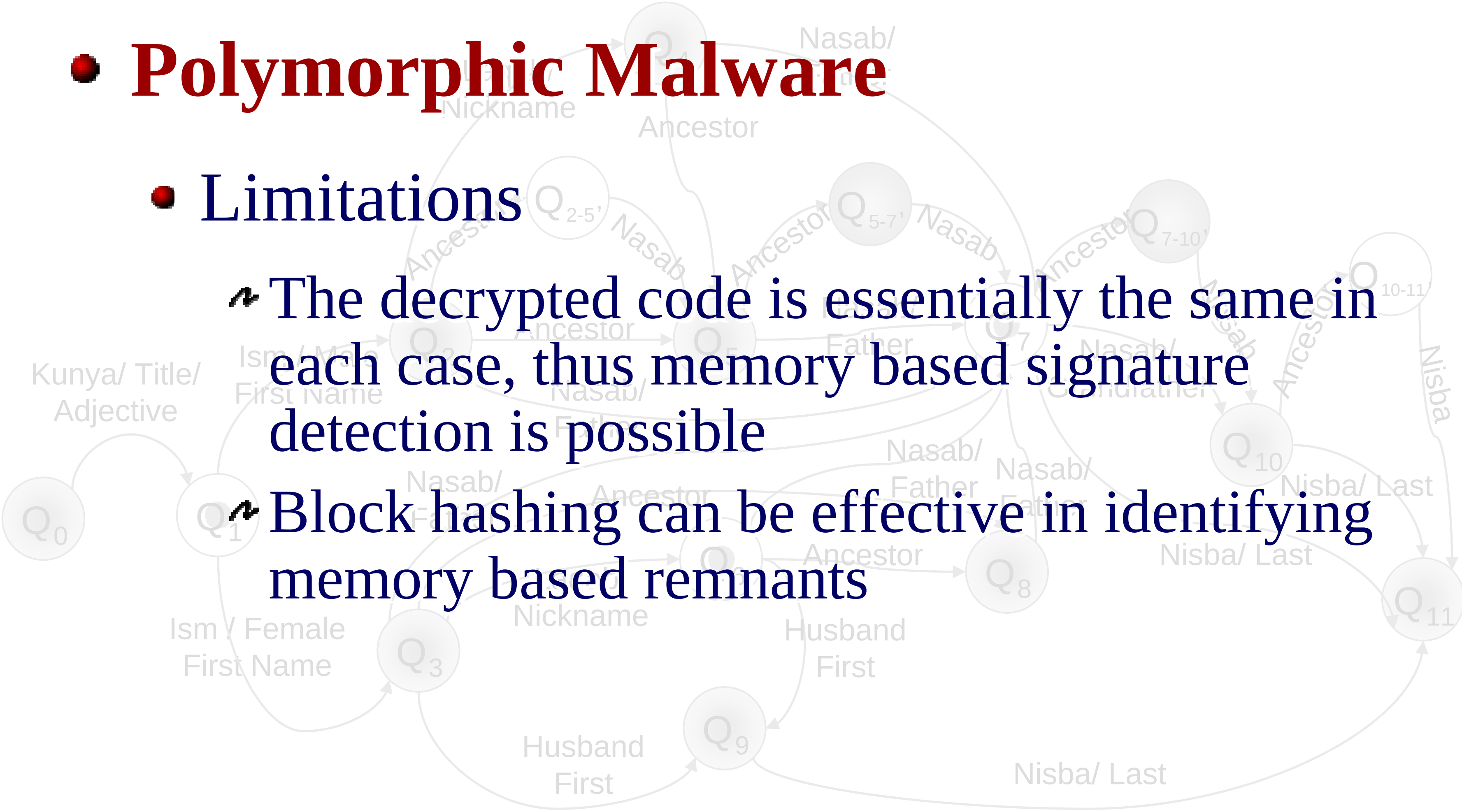


Overview and Definitions

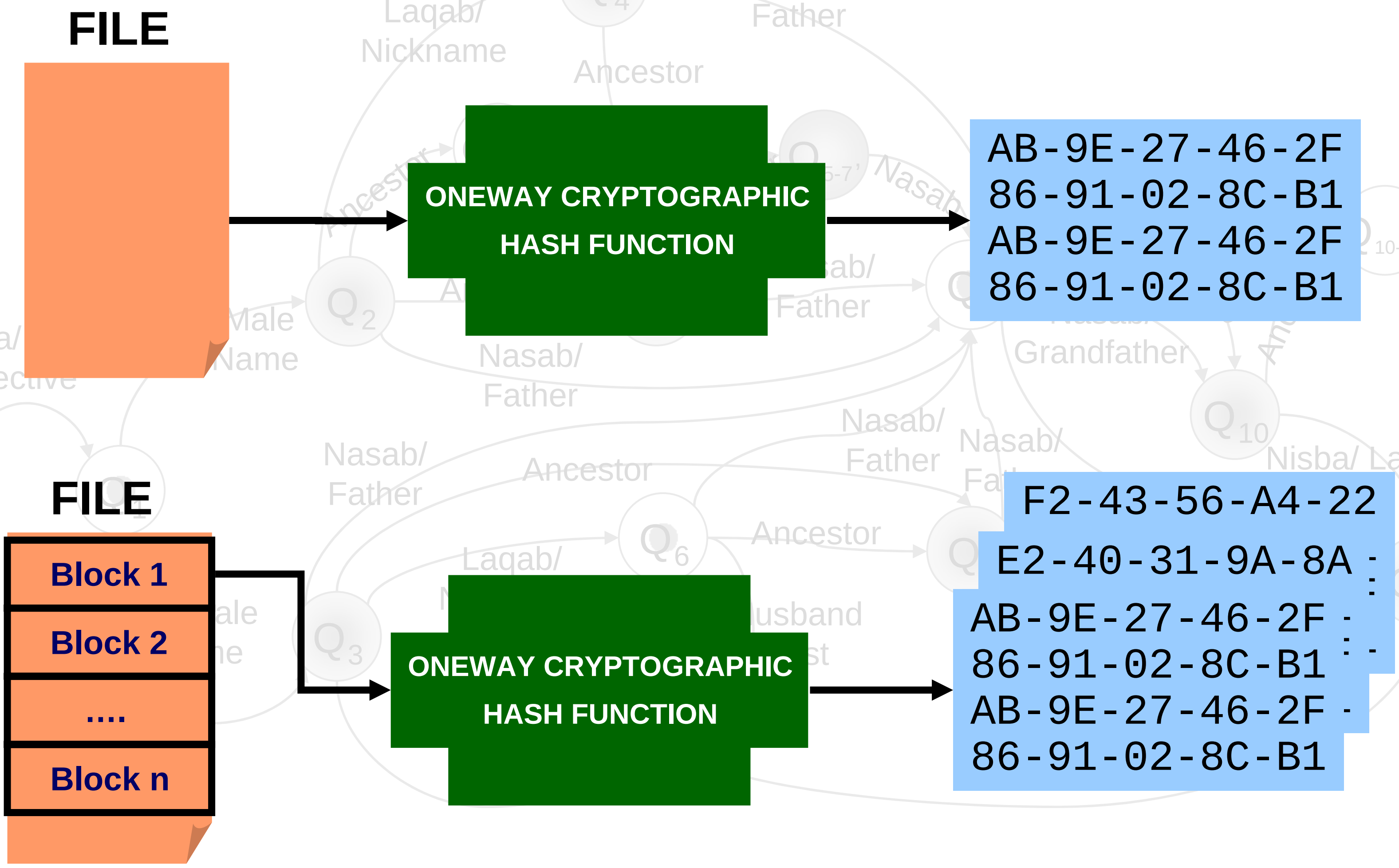
- **Polymorphic Malware**
  - Polymorphism loosely means: “change the appearance of”
  - Mutation Engines are bundled with the virus, worm or other self-propagating code
    - Common methods include
      - Encryption
      - Data appending / Data pre-pending

Overview and Definitions

- **Polymorphic Malware**
  - Limitations
    - The decrypted code is essentially the same in each case, thus memory based signature detection is possible
    - Block hashing can be effective in identifying memory based remnants



Memory Block Hashing



FILE

ONEWAY CRYPTOGRAPHIC HASH FUNCTION

AB-9E-27-46-2F
86-91-02-8C-B1
AB-9E-27-46-2F
86-91-02-8C-B1

FILE

Block 1

Block 2

....

Block n

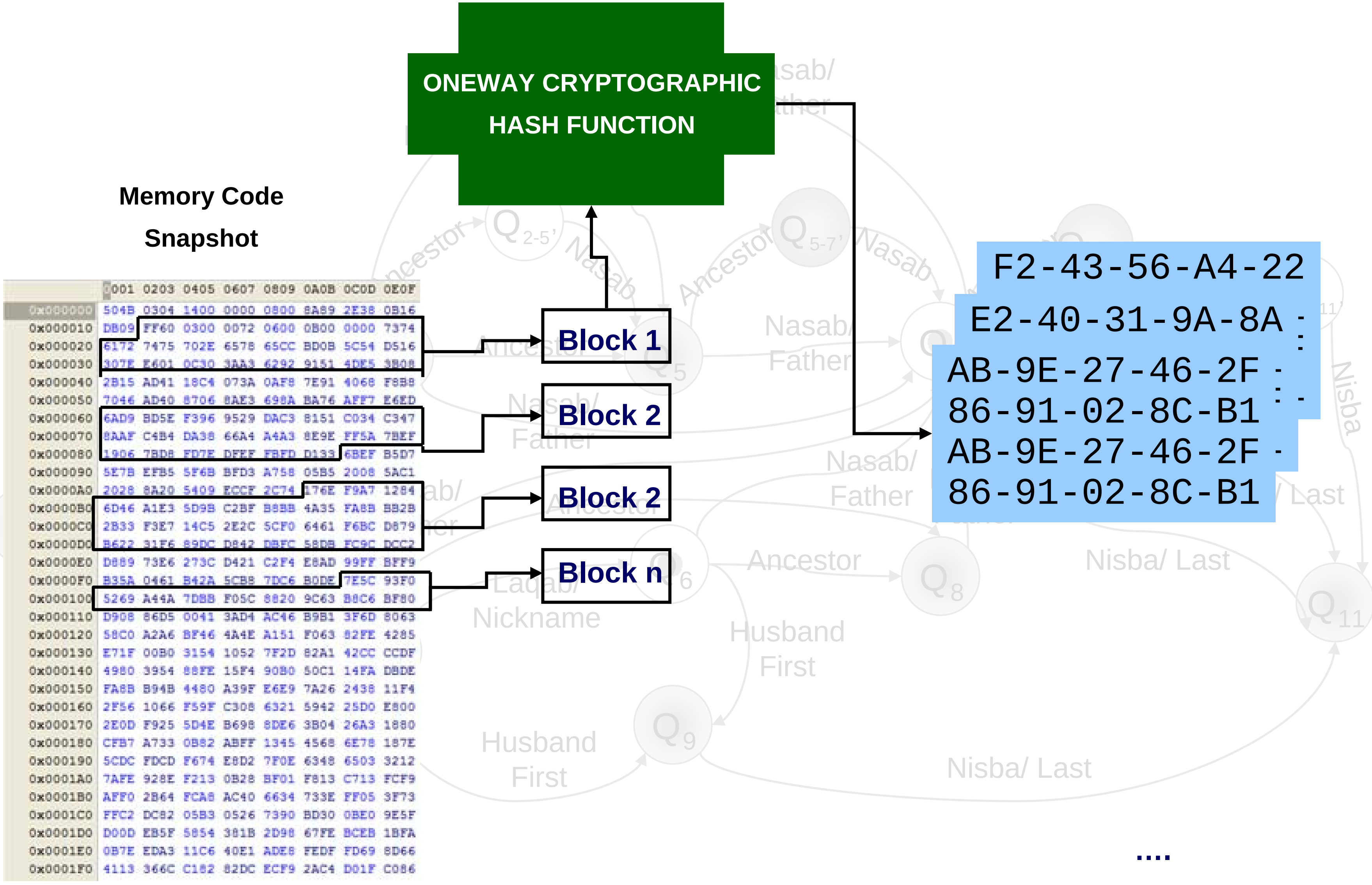
ONEWAY CRYPTOGRAPHIC HASH FUNCTION

F2-43-56-A4-22

E2-40-31-9A-8A

AB-9E-27-46-2F
86-91-02-8C-B1
AB-9E-27-46-2F
86-91-02-8C-B1

Memory Block Hashing



Memory Code Snapshot

```
         0001 0203 0405 0607 0809 0A0B 0C0D 0E0F
0x000000 504B 0304 1400 0000 0800 8A89 2E38 0B16
0x000010 DB09 FF60 0300 0072 0600 0B00 0000 7374
0x000020 6172 7475 702E 6578 65CC BD0B 5C54 D516
0x000030 307E E601 0C30 3AA3 6292 9151 4DE5 3B08
0x000040 2B15 AD41 18C4 073A 0AF8 7E91 4068 F8B8
0x000050 7046 AD40 8706 8AE3 698A BA76 AFF7 E6ED
0x000060 6AD9 BD5E F396 9529 DAC3 8151 C034 C347
0x000070 8AAF C4B4 DA38 66A4 A4A3 8E9E FF5A 7BEF
0x000080 1906 7BD8 FD7E DFEF FBFD D133 6BEF B5D7
0x000090 5E7B EFB5 5F6B BFD3 A758 05B5 2008 5AC1
0x0000A0 2028 8A20 5409 ECCF 2C74 176E F9A7 1284
0x0000B0 6D46 A1E3 5D9B C2BF B8BB 4A35 FA8B BB2B
0x0000C0 2B33 F3E7 14C5 2E2C 5CF0 6461 F6BC D879
0x0000D0 B622 31F6 89DC D842 DBFC 58D8 FC9C DCC2
0x0000E0 D889 73E6 273C D421 C2F4 E8AD 99FF BFF9
0x0000F0 B35A 0461 B42A 5CB8 7DC6 B0DE 7E5C 93F0
0x000100 5269 A44A 7DBB F05C 8820 9C63 B8C6 BF80
0x000110 D908 86D5 0041 3AD4 AC46 B9B1 3F6D 8063
0x000120 58C0 A2A6 BF46 4A4E A151 F063 82FE 4285
0x000130 E71F 00B0 3154 1052 7F2D 82A1 42CC CCDF
0x000140 4980 3954 88FE 15F4 90B0 50C1 14FA DBDE
0x000150 FA8B B94B 4480 A39F E6E9 7A26 2438 11F4
0x000160 2F56 1066 F59F C308 6321 5942 25D0 E800
0x000170 2E0D F925 5D4E B698 8DE6 3B04 26A3 1880
0x000180 CFB7 A733 0B82 ABFF 1345 4568 6E78 187E
0x000190 5CDC FDCD F674 E8D2 7F0E 6348 6503 3212
0x0001A0 7AFE 928E F213 0B28 BF01 F813 C713 FCF9
0x0001B0 AFF0 2B64 FCA8 AC40 6634 733E FF05 3F73
0x0001C0 FFC2 DC82 05B3 0526 7390 BD30 0BE0 9E5F
0x0001D0 D00D EB5F 5854 381B 2D98 67FE BCEB 1BFA
0x0001E0 0B7E EDA3 11C6 40E1 ADE8 FEDF FD69 8D66
0x0001F0 4113 366C C182 82DC ECF9 2AC4 D01F C086
```

ONEWAY CRYPTOGRAPHIC HASH FUNCTION

Block 1

Block 2

Block 2

Block n

F2-43-56-A4-22

E2-40-31-9A-8A

AB-9E-27-46-2F

86-91-02-8C-B1

AB-9E-27-46-2F

86-91-02-8C-B1

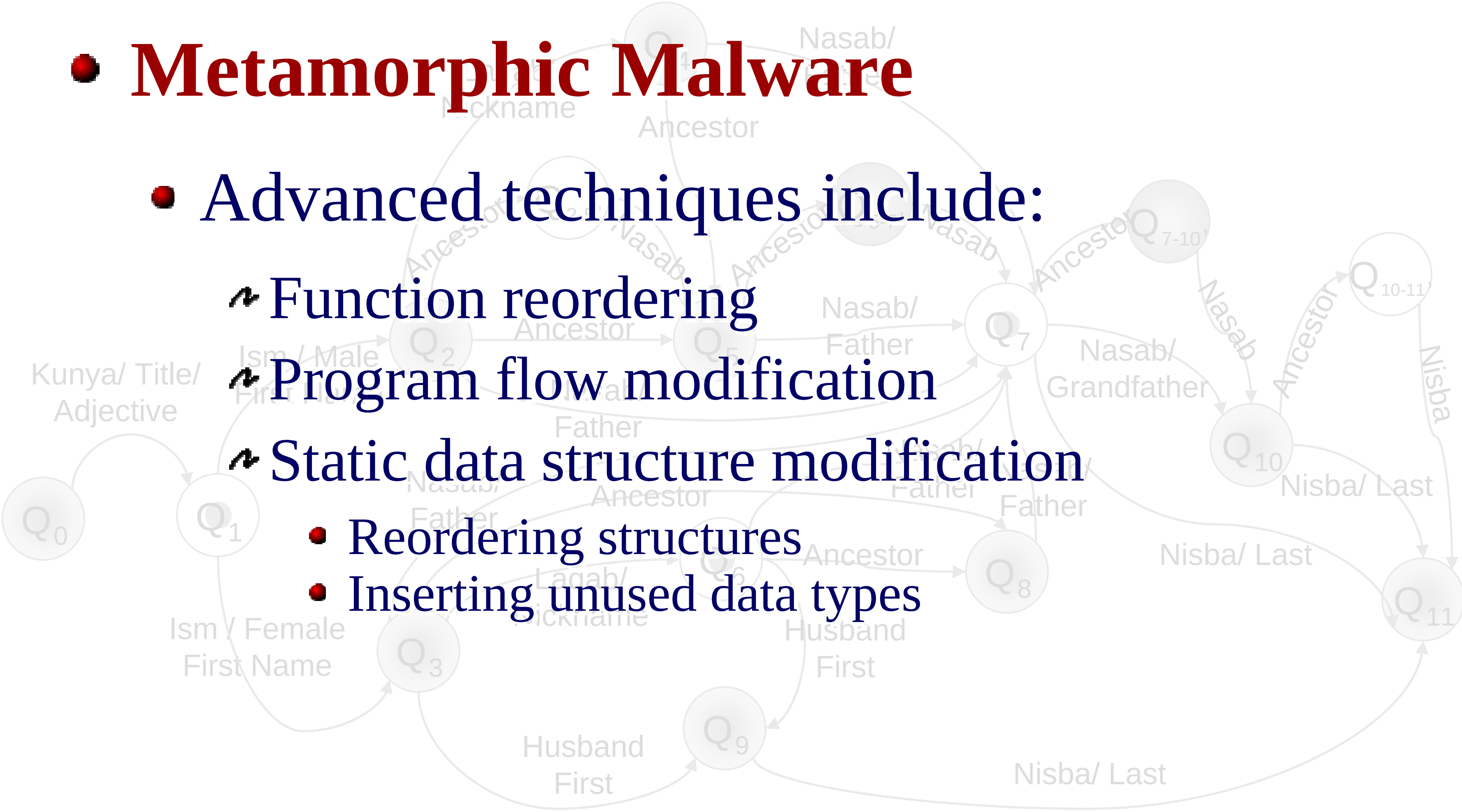
....

Overview and Definitions

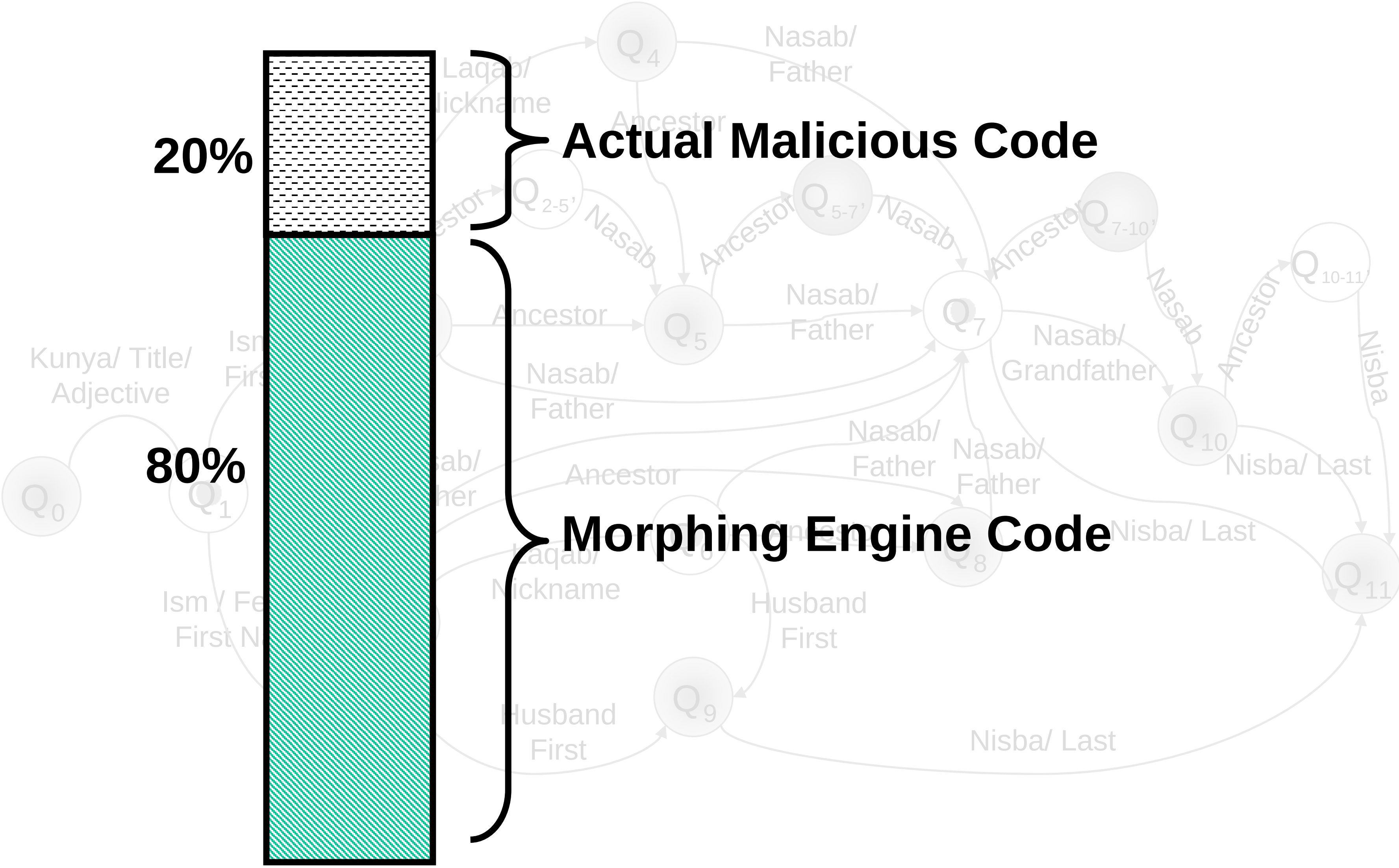
- **Metamorphic Malware**
  - Metamorphic Malware: “automatically re-codes itself each time it propagates or is distributed”
  - Simple techniques include:
    - Adding varying lengths of NOP instructions
    - Permuting use registers
    - Adding useless instructions and loops within the code segments

Overview and Definitions

- **Metamorphic Malware**
  - Advanced techniques include:
    - Function reordering
    - Program flow modification
    - Static data structure modification
      - Reordering structures
      - Inserting unused data types



Metamorphic Structure



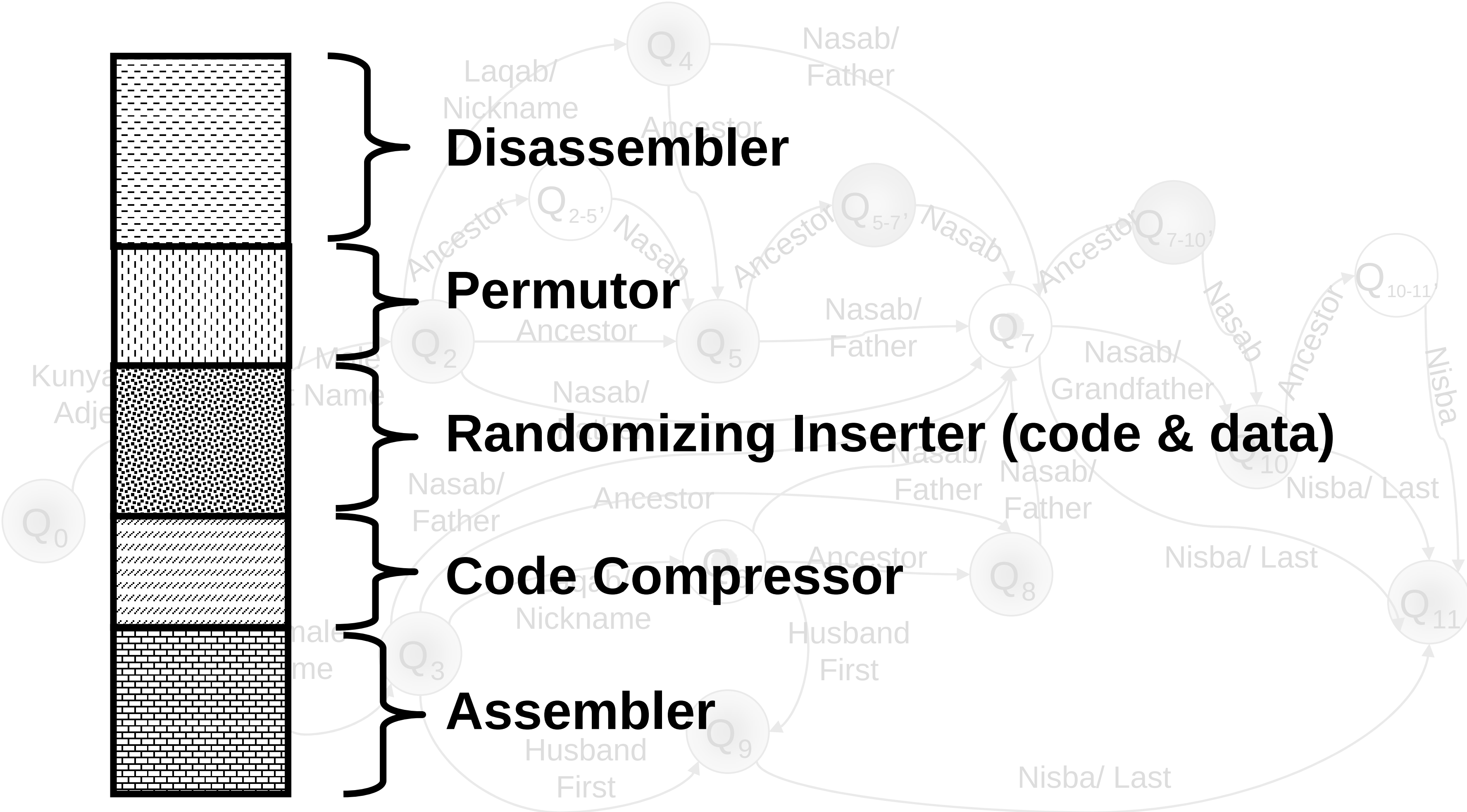
20%

Actual Malicious Code

80%

Morphing Engine Code

Morphing Engine Components



Disassembler

Permutor

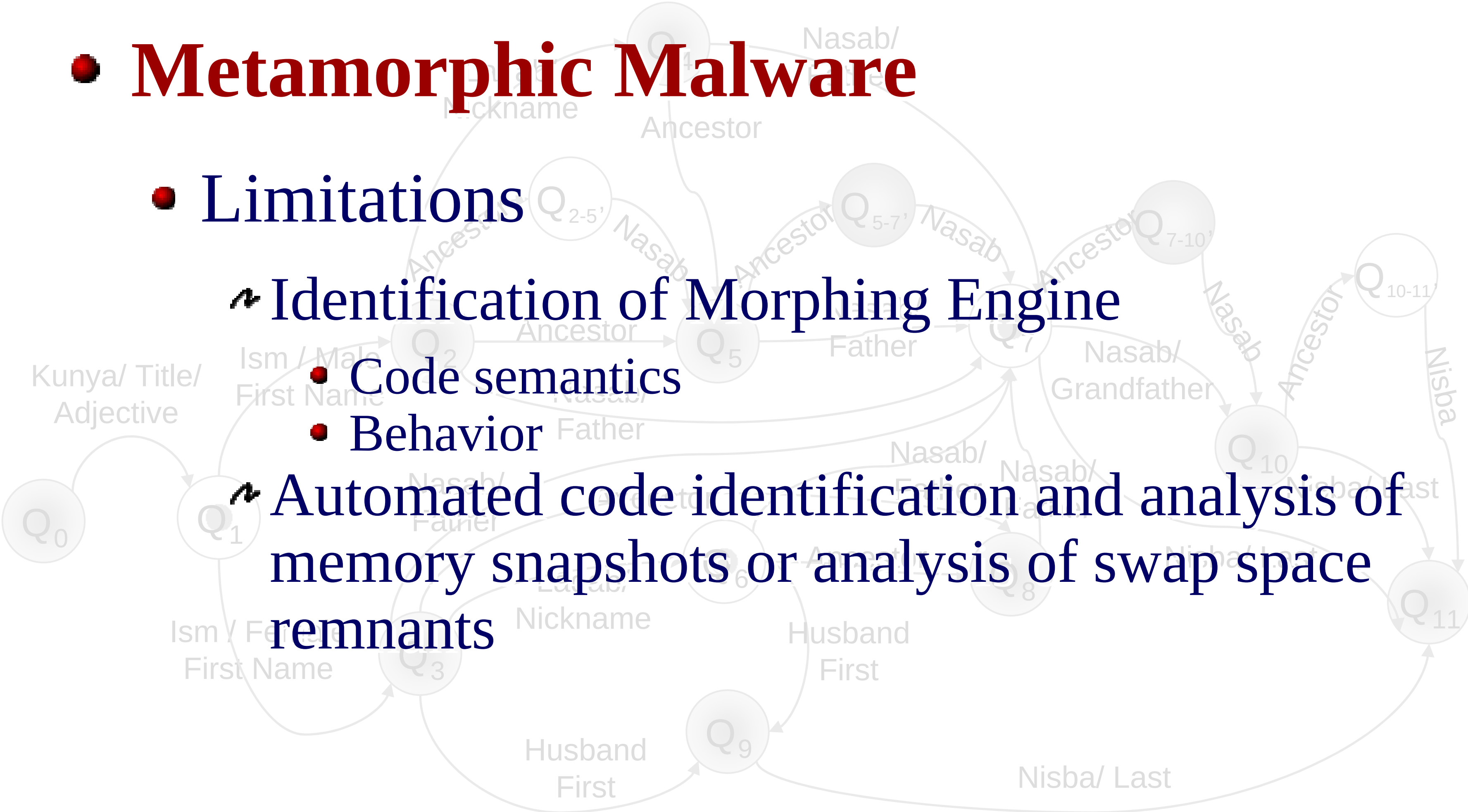
Randomizing Inserter (code & data)

Code Compressor

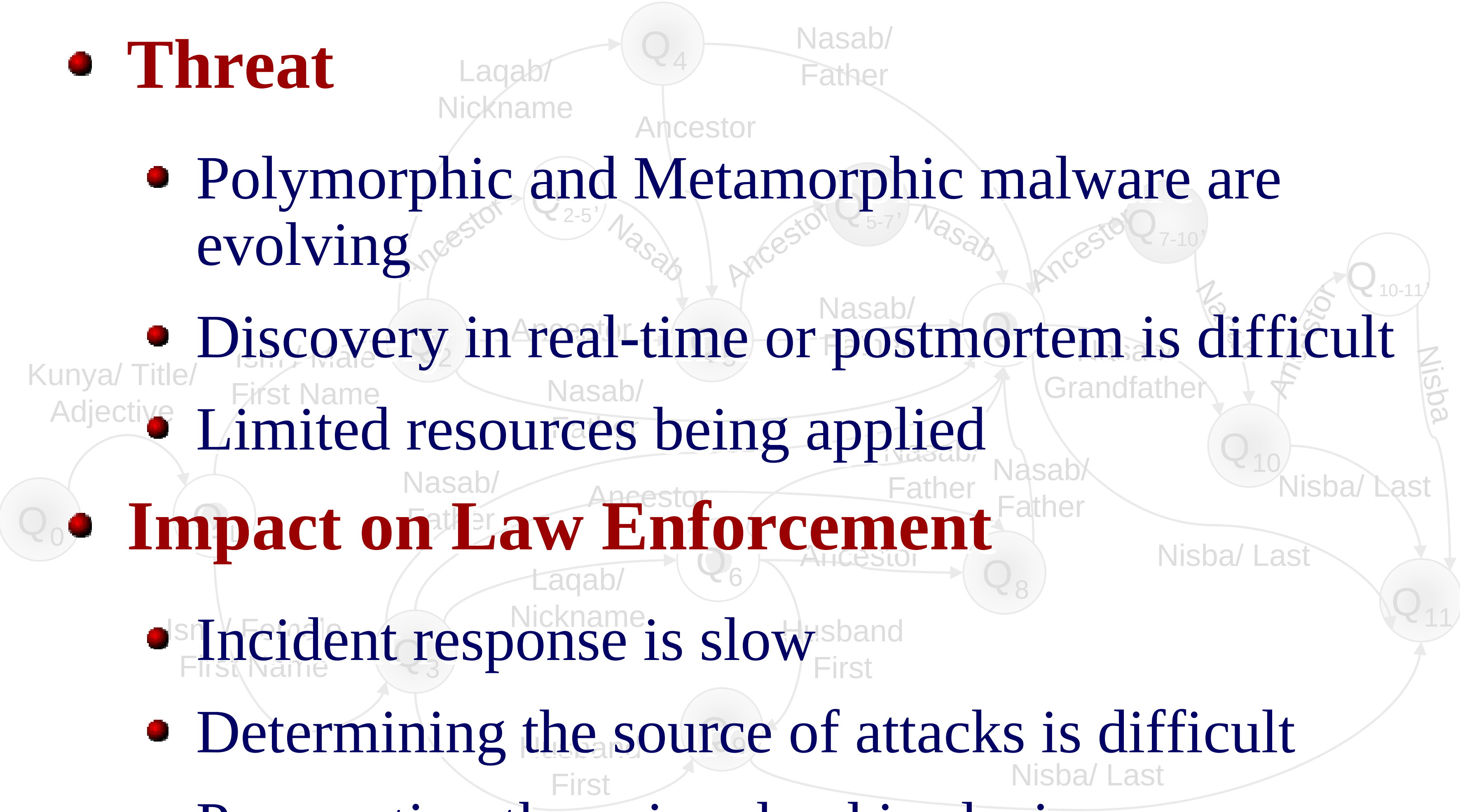
Assembler

Overview and Definitions

- **Metamorphic Malware**
  - Limitations
    - Identification of Morphing Engine
      - Code semantics
      - Behavior
    - Automated code identification and analysis of memory snapshots or analysis of swap space remnants

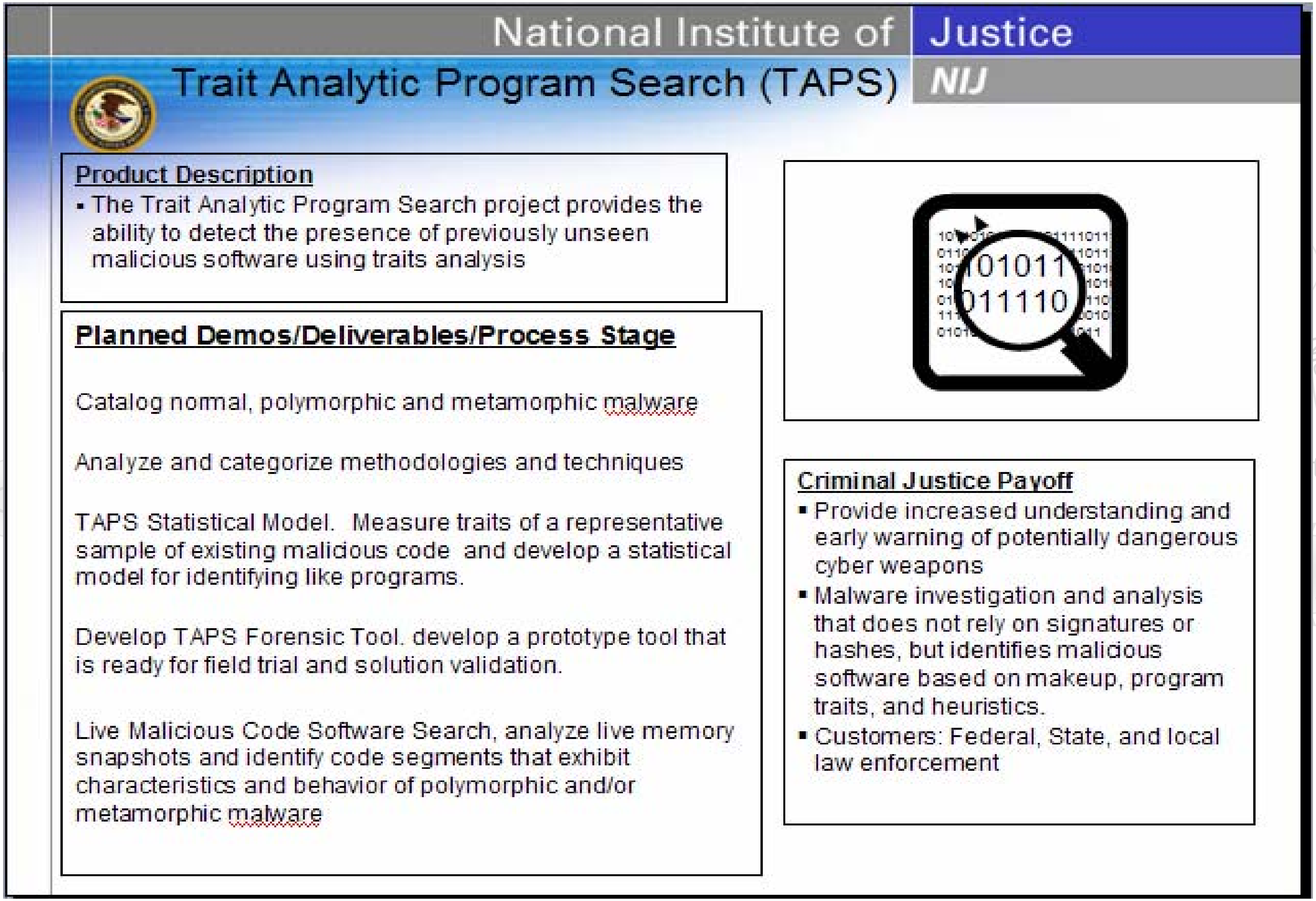


Summary



- **Threat**
  - Polymorphic and Metamorphic malware are evolving
  - Discovery in real-time or postmortem is difficult
  - Limited resources being applied
- **Impact on Law Enforcement**
  - Incident response is slow
  - Determining the source of attacks is difficult
  - Prosecuting those involved is elusive

Solution Development



National Institute of Justice

Trait Analytic Program Search (TAPS) NIJ

Product Description

- The Trait Analytic Program Search project provides the ability to detect the presence of previously unseen malicious software using traits analysis

Planned Demos/Deliverables/Process Stage

Catalog normal, polymorphic and metamorphic malware

Analyze and categorize methodologies and techniques

TAPS Statistical Model. Measure traits of a representative sample of existing malicious code and develop a statistical model for identifying like programs.

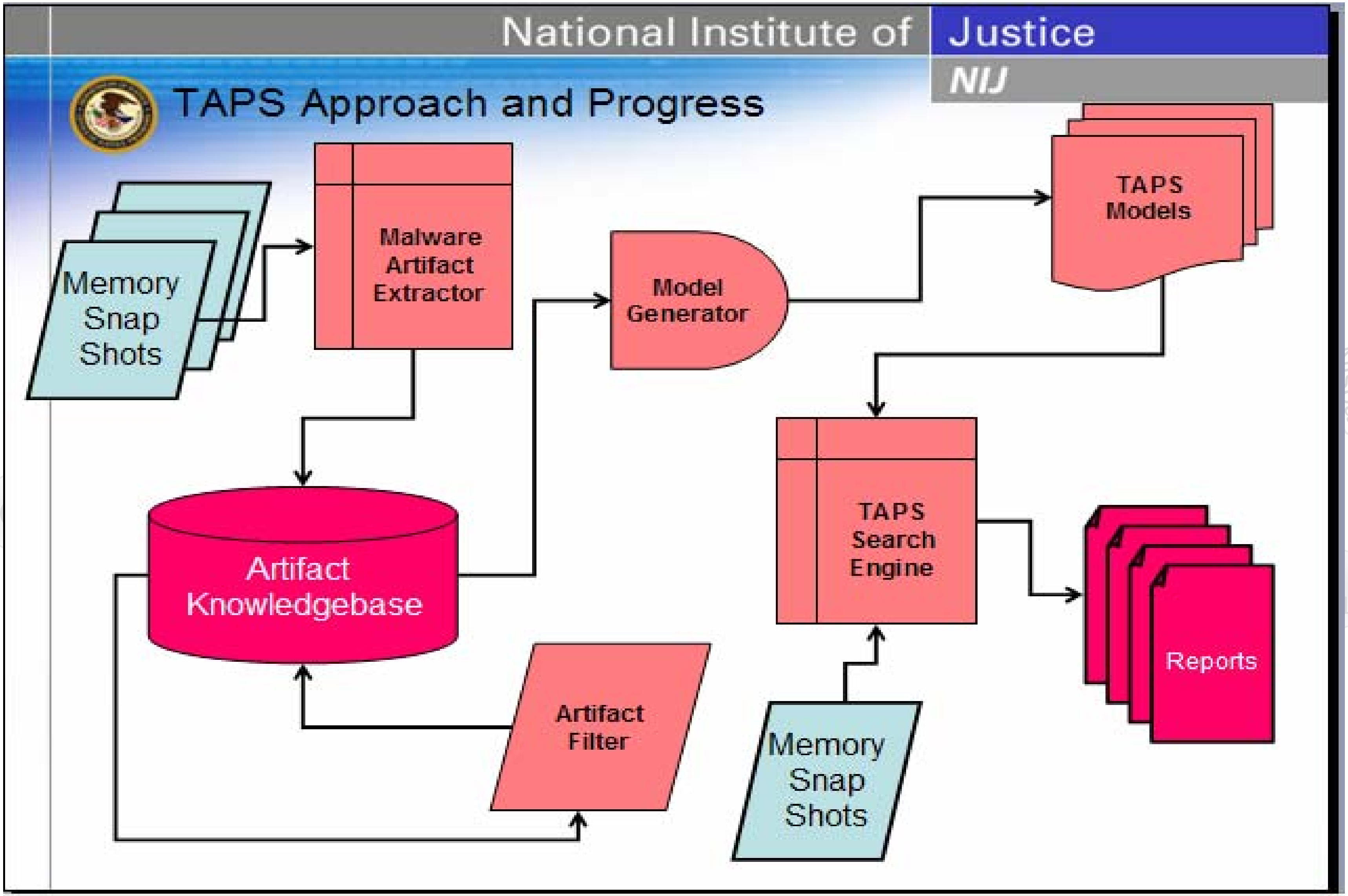
Develop TAPS Forensic Tool. develop a prototype tool that is ready for field trial and solution validation.

Live Malicious Code Software Search, analyze live memory snapshots and identify code segments that exhibit characteristics and behavior of polymorphic and/or metamorphic malware

Criminal Justice Payoff

- Provide increased understanding and early warning of potentially dangerous cyber weapons
- Malware investigation and analysis that does not rely on signatures or hashes, but identifies malicious software based on makeup, program traits, and heuristics.
- Customers: Federal, State, and local law enforcement

Solution Development



National Institute of Justice

NIJ

TAPS Approach and Progress

Memory Snap Shots

Malware Artifact Extractor

Model Generator

TAPS Models

Artifact Knowledgebase

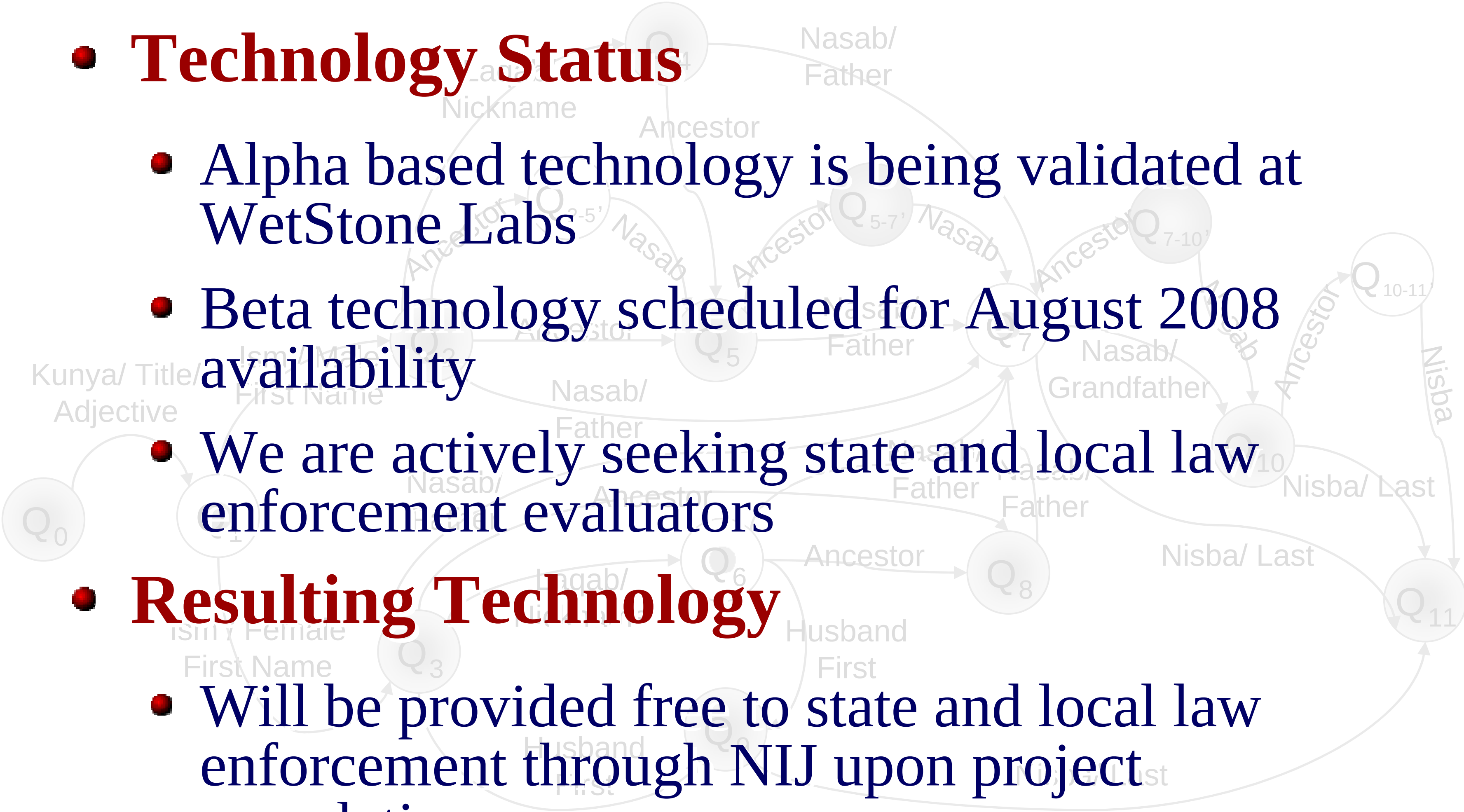
Artifact Filter

TAPS Search Engine

Memory Snap Shots

Reports

Next Steps / Opportunity



- ## Technology Status
  - Alpha based technology is being validated at WetStone Labs
  - Beta technology scheduled for August 2008 availability
  - We are actively seeking state and local law enforcement evaluators
- ## Resulting Technology
  - Will be provided free to state and local law enforcement through NIJ upon project completion