



# **A Review of Advancements in Code Breaking and Password Recovery Technology**



# Code Breaking and Digital Forensics

FBI Supervisory Special Agent

Chris Beeson

Laboratory Director

Silicon Valley Regional Computer Forensic Laboratory

Menlo Park, CA

[cbeeson@fbi.gov](mailto:cbeeson@fbi.gov)

[www.rcfl.gov](http://www.rcfl.gov)



# Course Content

- Basic concepts in Cryptography
- Keyspace Dilemma
- PRTK
- Rainbow Tables
- Other Code breaking tools



# What is Cryptography

- Cryptography: The art and science of keeping messages/information secure
- Encryption: Transformation of data into unreadable form
- Decryption: Reverse of encryption



# Types of Encryption

- Access Protection
  - Not encrypted, just locked
- Data obfuscation
  - Encryption by way of scrambling (ROT13)
  - Trillian
  - XOR
- Data encryption
  - Crypto systems



# Password States

- Not stored
  - Application uses authentication sequence to verify (ie Word/Excel)
- Stored by User
  - Application offers to store, then obfuscate or encrypt (IE, Yahoo, Netscape)
- Stored by Application
  - EFS



# Password Types

- Open/Modify Passwords (Word/Excel)
- Unlock
  - No encrypt, needed to open file (early Quicken)
- User/Master (PDF)
- Administrator
- Password archives
  - PasswordSafe, PasswordsPlus, etc

# Terminology

**Function**

Salt

FEK

Keyspace

Array

Plain Text

Cipher Text

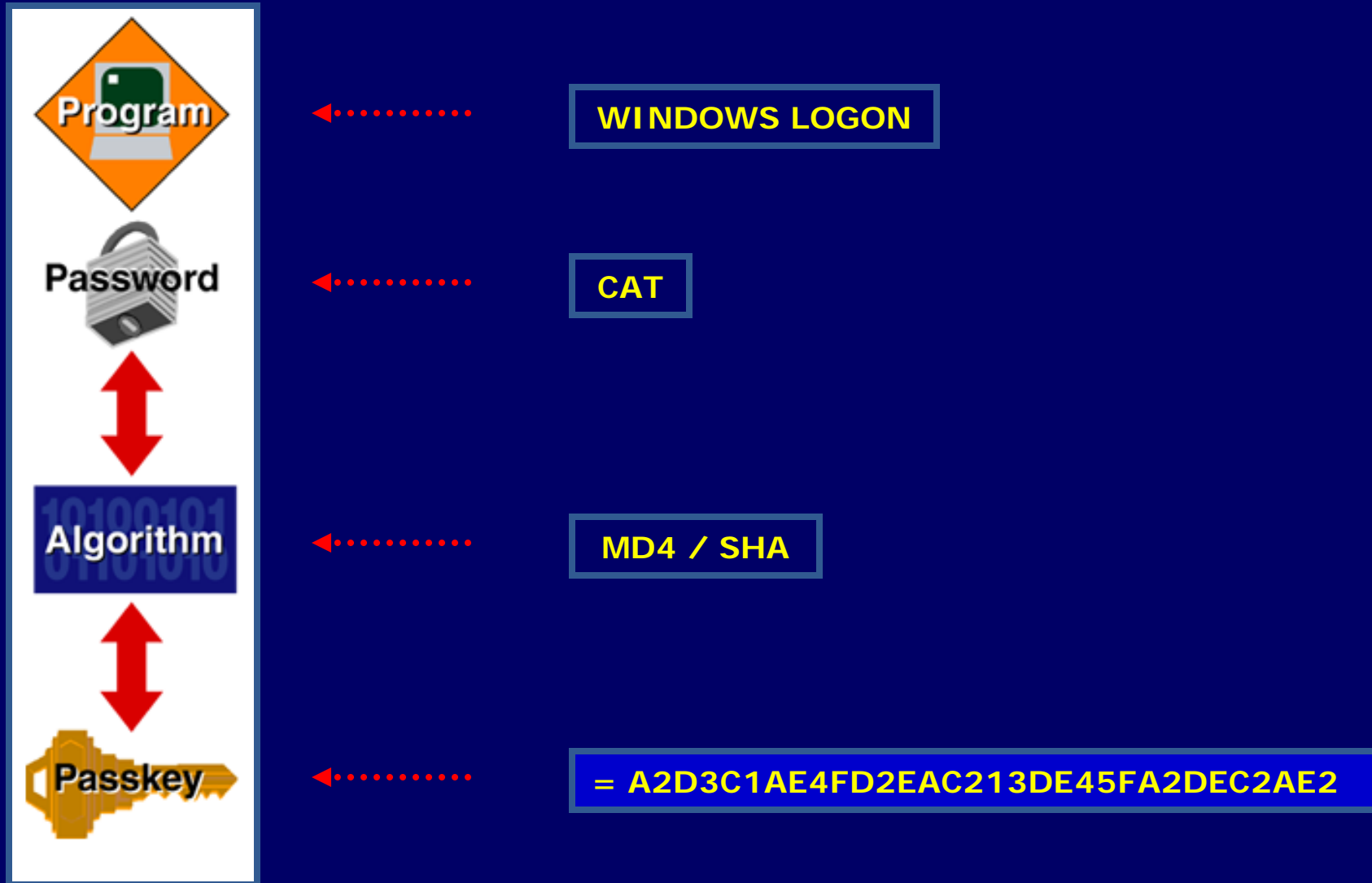




# Hash

- Hash Function
  - Variable length data stream = fixed length number
  - Must be reproducible with same data
  - Cannot be reversed (number back to original data)
  - Also called Message Digests (ie md5)

# What is a Hash Function?



# Terminology

Function

**Salt**

FEK

Keyspace

Array

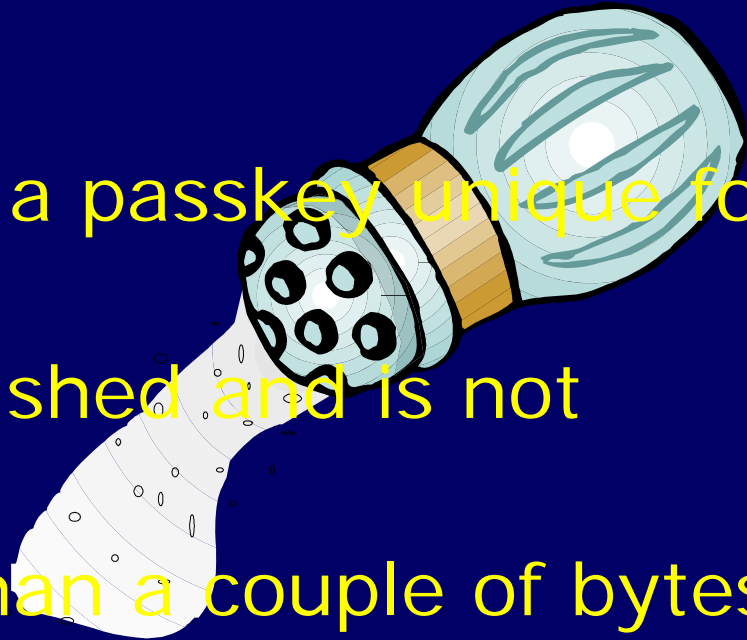
Plain Text

Cipher Text



# Salt

- Salt is used to make a passkey unique for each user/machine
- Salt is normally published and is not secret
- Salt is rarely more than a couple of bytes in size



## Two Users – Same Password - With Salt:

User 1 cat = f3fca383b05f665ff43244ecdecfe959

User 2 cat = ccd15a3c85d28019fb3ef173f7ff344a

# Terminology

Function

Salt

**FEK**

Keyspace

Array

Plain Text

Cipher Text

# File Encryption Key



+ SALT

+



||

9o2GrDE398fD7ipR3

*You get the idea !*

# Terminology

Function

Salt

FEK

**Keyspace**

Array

Plain Text

Cipher Text



# Keyspace Values

Key: **Any One of a Larger Number of Values**

Keyspace: **Range of Possible Values**

(this can get big!)

20	1,048,576
30	1,073,741,824
32	4,294,967,296
33	8,589,934,592
40	1,099,511,627,776
50	1,125,899,906,842,620
56	72,057,594,037,927,900
60	1,152,921,504,606,850,000
70	1,180,591,620,717,410,000,000
80	1,208,925,819,614,630,000,000,000
90	1,237,940,039,285,380,000,000,000,000
100	1,267,650,600,228,230,000,000,000,000,000
110	1,298,074,214,633,710,000,000,000,000,000,000
120	1,329,227,995,784,920,000,000,000,000,000,000,000
128	340,282,366,920,938,000,000,000,000,000,000,000,000
160	1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000





# Keyspace

Key Space Calculation Spreadsheet	
Key Space (# of bits)	40
Size of Key Space	1,099,511,627,776
Keys Tested Per Second	500,000
# of Machines	1
Time (in seconds)	2,199,023
Time (in hours)	610.840
Time (in days)	25.45
Time (in years)	0.070

# Terminology

Function

Salt

FEK

Keyspace

**Array**

Plain Text

Cipher Text



# Array

An Array is used by cryptographic systems to generate bit streams used to encrypt and decrypt data.

A random bit is used with a “Exclusive Or” (XOR) algorithm that switches the bits that comprise the data.

# Terminology

Function

Salt

FEK

Keyspace

Array

**Plain Text**

**Cipher Text**

# Plain Text → Cipher Text

```
Plain Text - Notepad
File Edit Format View Help
This is the Plain Text file

It will be XOR'd against the
binary result of the array
manipulation output

The result will be cipher Text

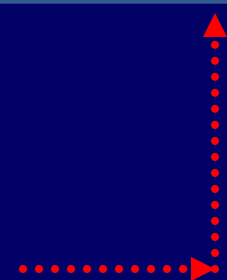
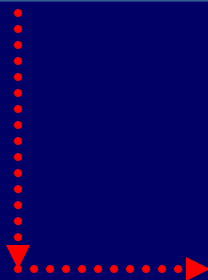
As we learn about XOR - if we
can figure out the pattern - it
changes the story. This is why
passwords must be unique !
```

```
Cipher Text - Notepad
File Edit Format View Help
fhr03jnxk39vns1nv49bnsn2

2e0vnsvmj493jgsnb32vbkf9b
sdk230b5nvsksn38958ghwnv2
swdkj20vnween

349gut5jhwnvnwke02uv2vn2k4

2ngf0rv832vs1kjdkjw92hjfne
svw08enjvnwkjn025bn8cnv20vb
vw0v0rv38jvgje29vnn2kjdfne8
v82wv82jvkjsnsmw82jn5nvnv1v
```



**10100100001010011**  
(array value)  
**PT ^ array value = CT**

# Crypto System

Password

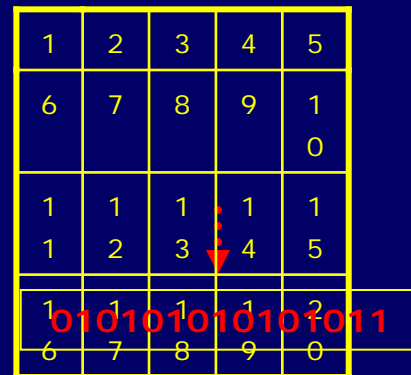


MD5 Hash, SHA Hash ??



MD5 Hash, SHA Hash ??

FEK



^ PT



```
Plain Text - Notepad
This is the Plain Text file
It will be XOR'd against the
binary result of the array
manipulation output
The result will be Cipher Text
As we learn about XOR - if we
can figure out the pattern - it
changes the story. This is why
passwords must be unique !
```



```
Cipher Text - Notepad
fhr03jnxk39vns1nv49bnsn2
2e0vnsvmj493jgsnb32vbkf9b
sdk230b5nvsksn38958ghwnv2
swdkj20vnween
349gut5jhwvvnwke02uv2vn2k4
2ngf0rv832vslkjdkjw92hjfne
svw08enjvwnkjn025bn8cnv20vb
vw0v0rv38jygje29vvn2kjdfne8
v82wv82jvkjsnsmw82jn5vnnv1v
```



# The Key Space and Password Space Dilemma



# Code Breaking Tools





# Password Cracking

Ability to recover passwords from well-known applications

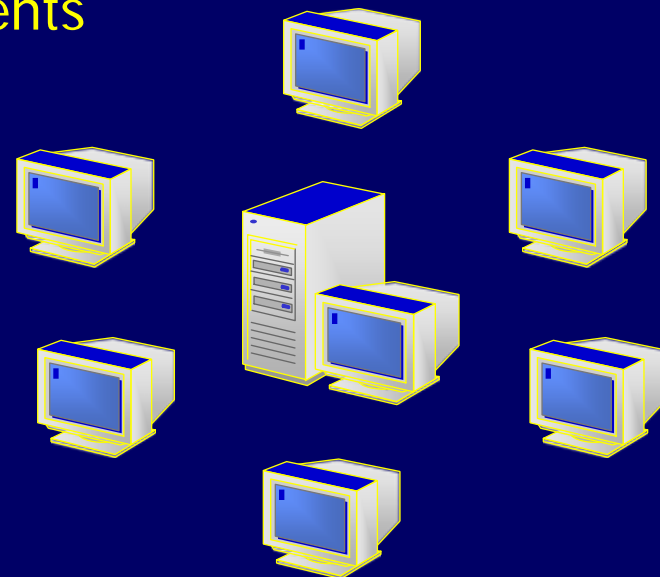
- Decrypt files, folders, and hard drives
- Gain access to files protected by the Microsoft Encrypted File System (EFS)



# Distributed Code Breaking

Ability to recover passwords and/or keys using:

- Brute-Force attacks - Key-Space attacks - Pass-phrase attacks
- One system manages many Clients
- Distributed code breaking to many clients
  - Apple Macintosh
  - Linux
  - UNIX
  - Windows
- Uses 'Idle Process' time





# **Attacking the RC4 Implementation in MS Office**



# Microsoft Office 40-bit Encryption

- Due to U.S. Export laws, MS Office 97 and later versions use 40-bit FEK to initialize RC4 symmetric encryption algorithm.
- An exhaustive key space attack of a 40-bit key using a 25 computer distributed network attack (DNA) takes 24+ hours



# MS Word – 40 bit Encryption

The image shows a screenshot of the Microsoft Word Security dialog box. The main dialog box has a title bar with a question mark and a close button. It contains several sections: "File encryption options for this document" with a "Password to open:" field containing "\*\*\*\*\*" and an "Advanced..." button; "File sharing options for this document" with a "Password to modify:" field; a "Read-only recommended" checkbox; a "Digital Signature" button; "Privacy options" with "Remove" and "Warn on change" checkboxes, and a checked "Store" checkbox; and "Macro security" with an "Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers." button. Overlaid on top of the main dialog is a smaller "Confirm Password" dialog box with a title bar, a "Reenter password to open:" field containing "\*\*\*\*\*", and "OK" and "Cancel" buttons. Red circles highlight the "Password to open:" field in the main dialog and the "Reenter password to open:" field in the sub-dialog.



# MS Word Advanced Encryption Option

The image shows a screenshot of the Microsoft Word Security dialog box. The "Security" dialog box is open, showing the "File encryption options for this document" section. The "Password to open" field contains "\*\*\*\*" and is circled in red. To its right is an "Advanced..." button. Below this is the "File sharing options for this document" section, with a "Password to modify" field. In the foreground, the "Encryption Type" dialog box is open, showing a list of encryption options. The "RC4, Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)" option is selected. Below the list is a "Choose a key length" field set to "128" and a checked "Encrypt document properties" checkbox. The "Encryption Type" dialog box has "OK" and "Cancel" buttons at the bottom. The "Security" dialog box also has "OK" and "Cancel" buttons at the bottom.

# Code Breaking Tools

- AccessData
  - Password Recovery Tool Kit (PRTK)
  - Distributed Network Attack (DNA)

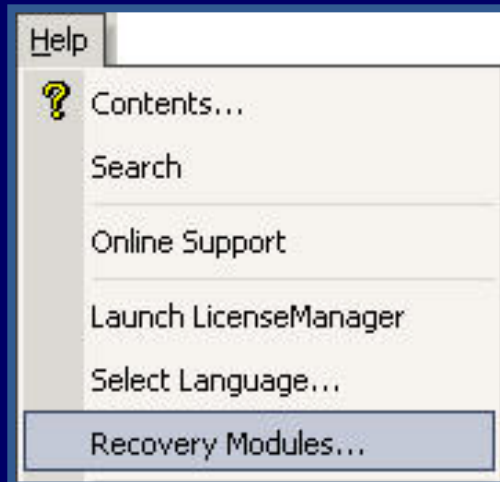
# PRTK Overview

The screenshot displays the AccessData Password Recovery Toolkit 6 application window. The title bar reads "AccessData Password Recovery Toolkit 6". The menu bar includes "File", "Edit", "View", "Analyze", "Tools", and "Help". The toolbar contains icons for file operations and analysis. The main window is divided into a file list on the left and a results table on the right. The "Help" menu is open, showing options like "Contents...", "Search", "Online Support", "Launch LicenseManager", "Select Language...", "Recovery Modules...", and "About PRTK".

Filename	Status	Results
C:\Documents and Settings\Dustin ...	Finished	1234AD1234
C:\Documents and Settings\Dustin ...	Finished	password Attack
C:\Documents and Settings\Dustin ...	Running	A>
C:\Documents and Settings\Dustin ...	Running	A>
C:\Documents and Settings\Dustin ...	Finished	password Attack
C:\Documents and Settings\Dustin ...	Finished	password Attack
C:\Documents and Settings\Dustin ...	Finished	supernova
C:\Documents and Settings\Dustin ...	Finished	Microsoft Word 97/2000 Password Attack
C:\Documents and Settings\Dustin ...	Finished	Microsoft Word 97/2000 Password Attack
C:\Documents and Settings\Dustin ...	Finished	Microsoft Word 97/2000 Password Attack
C:\Documents and Settings\Dustin ...	Finished	ZIP dictionary attack
C:\Documents and Settings\Dustin ...	Finished	ZIP dictionary attack
C:\Documents and Settings\Dustin ...	Finished	Mozilla Obfuscated Data



# Recovery Modules



Module Name	Display Name	Attack Types	Supported Products
Access	MS Access Password Module	decryption	Product Name: Microsoft Access Versions supported: <i>Unknown</i>
ACT	ACT! Password Module	decryption	Product Name: ACT! Versions supported: 1 - 4 2000 5 - 6
AIM	AIM Password Module	dictionary	Product Name: AOL Instant Messenger Versions supported: Through 5.5
AmiPro	AmiPro Password Module	dictionary	Product Name: Ami Pro Versions supported: <i>Unknown</i>
AOL	AOL Password Module	keyspace decryption	Product Name: AOL Versions supported: 8.0 - 9.0
Approach	Lotus Approach Password Module	decryption	Product Name: Lotus Approach Versions supported: Through 97
ARJ	ARJ Password Module	dictionary keyspace	Product Name: ARJ Versions supported: Through 2.82
Ascend	Ascend Password Module	decryption	Product Name: Ascend Versions supported: <i>Unknown</i>
BestCrypt	BestCrypt Password Module	dictionary	Product Name: BestCrypt Versions supported: 4.x - 7.x

**Some up front knowledge might make a difference !!**

ABICoder	InvisibleSecrets	ProtectedRegistry
Access	Justsystem	ProWrite
ACT	Kaikei	PST
AIM	Keepass	PWL
AmiPro	Kremlin	QuattroPro
AOL	Lockit	Quickbooks
Approach	Lotus123	Quicken
ARJ	MaxCrypt	RARPassword
Ascend	MessengerPlus	SafeHouse
Ashampoo	Money	SAMFile
BestCrypt	MozillaMasterPassword	Scheduler
BPFTP	MozillaProtectedData	ScreenSaver
CDLock	MSBackup	SecretStuff
CheckWriter	MSMail	SecureIT
CodedDrag	MSNMessenger	SiFEU
crypt	MYOB	SourceSafe
Cryptainer	NetscapeMail	Steganos
CryptaXix	office	STools
Cryptext	Omziff	SymantecQA
CuteFTP	OpenOffice	VBA
DataPerfect	Organizer	VersaCheck
dBASE	Palm	Whisper
DriveCrypt	Paradox	WinZip9
DriveCryptPP	PasswordPal	WordPerfect
EasyCrypto	PasswordSafe	WordPro
EFS	PCEncrypt	WS_FTP
EMF	PDF	XPCredentials
FileMaker	PFX	YahooMessenger
Hello	PGP	ZIP
ICQ	PGPDisk	



- Working Smarter rather than Harder!

# Dictionary Attacks

- User Created – Inside/Outside PRTK
- Dictionaries
  - Common – Common English words
  - Passwords – Password lists (golden dictionary)
  - Crime – Sex and drugs
  - Misc – Keyboard combinations
  - Names – Common names
  - General – Webster like
  - Unicode

# Dictionary Creation

Generating phrases...



Processing completed!

Cancel

OK

## Dictionary

Dictionary...

Levels...

Profiles...

Find... Ctrl+F

Find Next Ctrl+N

Select All Ctrl+A

Preferences...

AccessData Dictionary Utility

Dictionary Tools Text Tools Help

### Standard Dictionary Generator

Select a source file:

Dictionary S

Language:

ENGLISH

Include:

Letters

Digits

Symbols

Diacritics

Description

ID Theft 3-en-c.adf

ID Theft 3-en-u.adf

indexDAT file notes-en-c.adf

indexDAT file notes-en-u.adf

Pass Phrases-en-c.adf

Pass Phrases-en-u.adf

[AR-1] Names-ar-c.adf

[AR-1] Names-ar-u.adf

[AR-2] Quran-ar-c.adf

[AR-2] Quran-ar-u.adf

[AR-3] General-ar-c.adf

[AR-3] General-ar-u.adf

[DE-1] General-1-de-c.adf

[DE-1] General-1-de-u.adf

# What is a Level?

- Level Technology – PRTK/DNA
- Primary Dictionary Search
  - rabbit
  - RABBIT
  - Rabbit
  - rABBIT
- 1abduct
- Toabduct
- abduct123

**Prefixes**

**Postfixes**

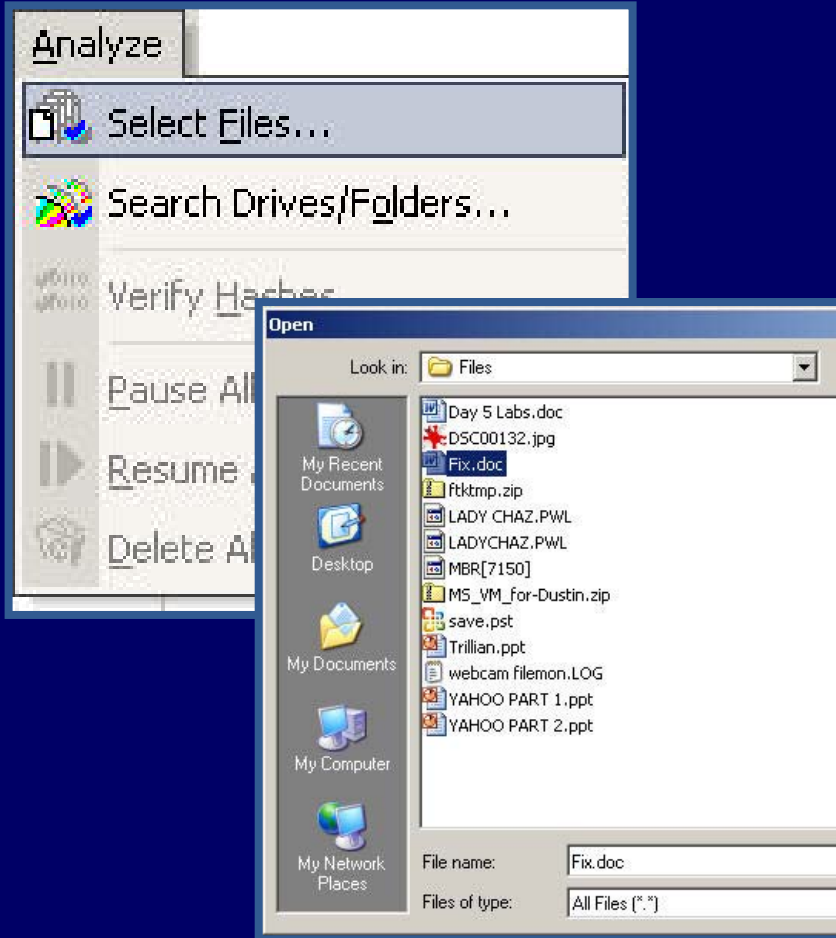
**Word in a Word**

**Concatenation**

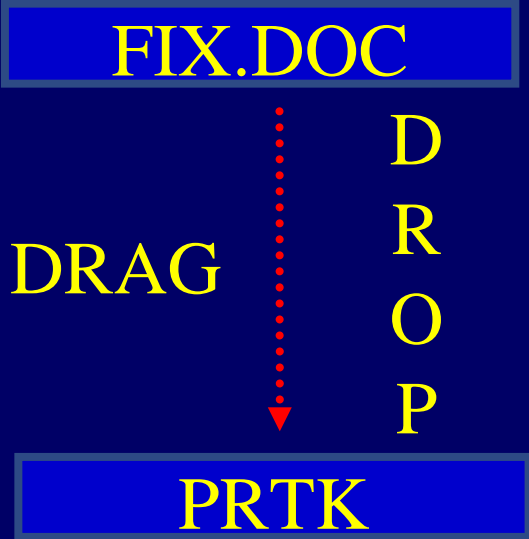
**Markov**

**Reverse**

# Starting a Job

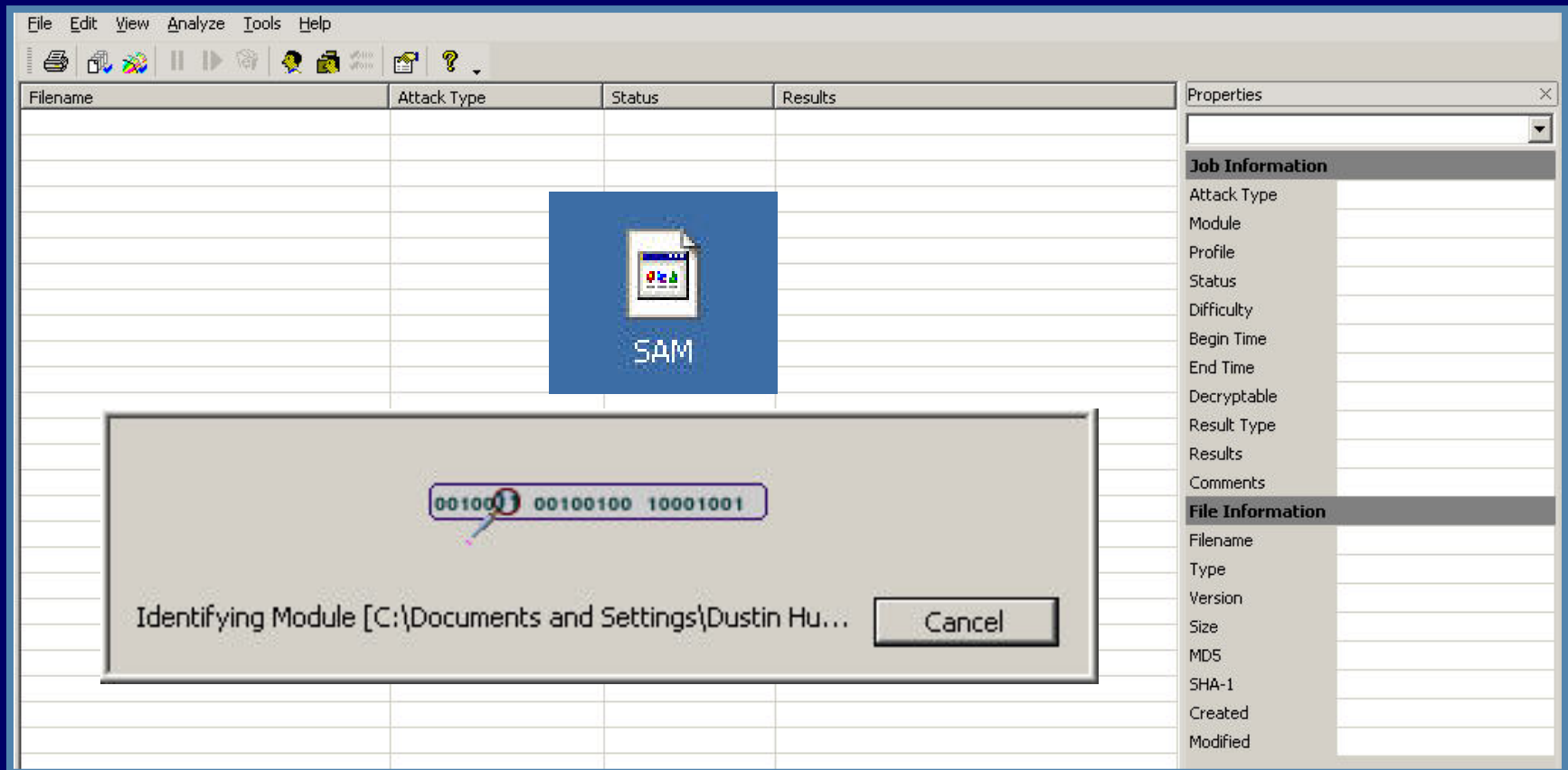


OR



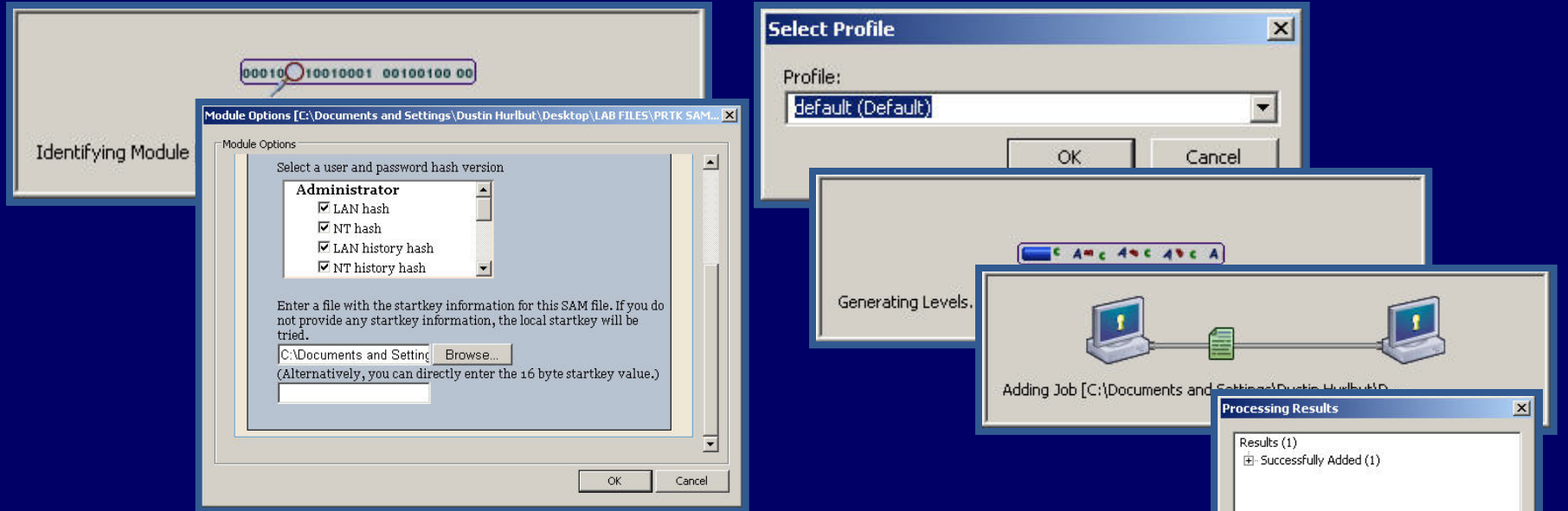
# Starting a Job – PRTK

- Drop file into PRTK





# Decryption Steps



Filename	Attack Type		
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [LAN history hash]		
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [LAN hash]	Waiting On	
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [NT hash]	Running	
C:\Documents and Settings\...	SAM user: VUSR_PHILLIP2000 [NT history hash]	Running	
C:\Documents and Settings\...	SAM user: Administrator [NT history hash]	Finished	giraffe
C:\Documents and Settings\...	SAM user: TsInternetUser [LAN hash]	Waiting On	
C:\Documents and Settings\...	SAM user: TsInternetUser [NT hash]	Running	
C:\Documents and Settings\...	SAM user: Administrator [NT hash]	Finished	giraffe

# Properties – Information

## Basic File and Status Information

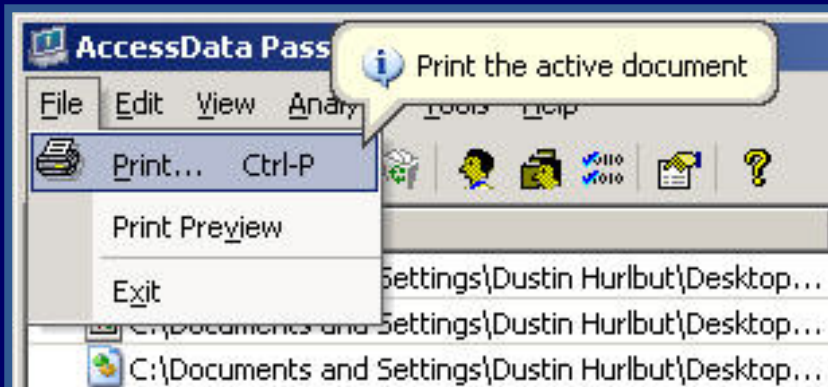
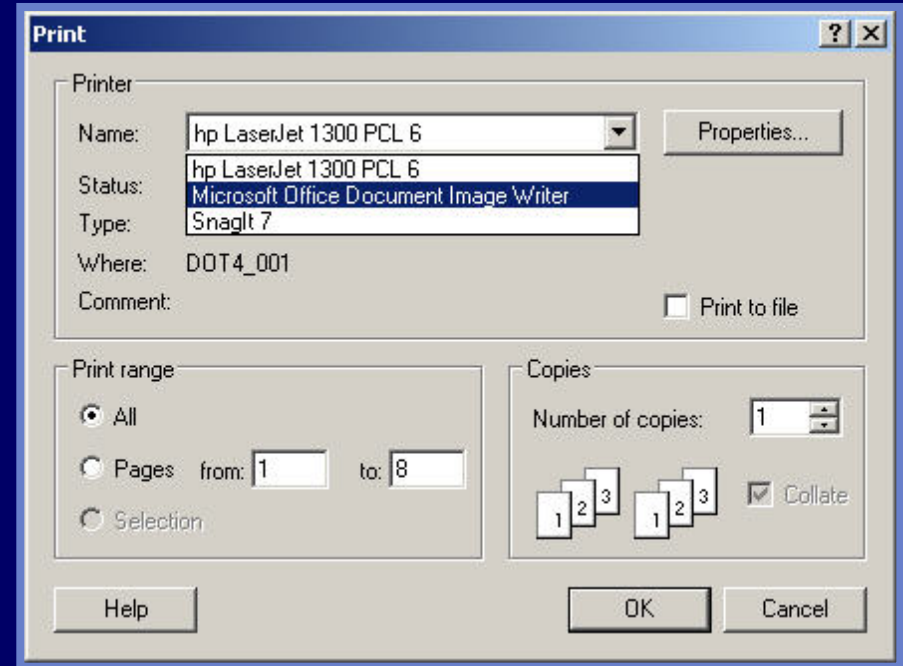
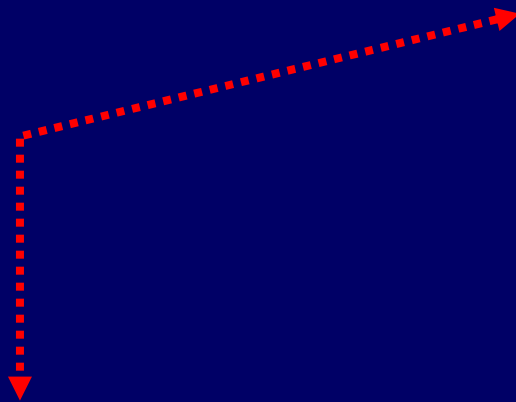
- File Name / Path
- Application Type
- Version
- Size
- Dates
- Hashes
- Attack Type
- Profile in use
- Status
- Time Begin / End

The screenshot shows the 'Properties' dialog box for a file named 'D:\AD NEW CD\LAB FILES\ENCRYP'. The 'Information' tab is selected. The 'File Information' section shows the filename, type (Word), version (2000), size (19456), and creation/modification dates. The 'Properties' section shows the attack type as 'Microsoft Word 97/2000 Password Attack' and the status as 'Finished'. The 'Results' section shows a table with search results.

Type	Data	Description	Found In
Password	اوب_ذك	Save As	(BAS-2-17) Dictionary primary search
Password	اوب_ذك	Write Reservation	

# Documenting Results – PRTK

- Written Reports
- Electronic Reports



# Documenting Results – PRTK

C:\Documents and Settings\Dustin Hurlbut\Desktop\Encrypted Files\Sagan\Was Einstein Right.doc

.....Commonly Registered Type: Microsoft Word Document

.....Identified Type: Word

.....Password                      gravity

Page 2 of 9

---

*PRTK REPORT      07/15/05*

Description:

Save As

Found In

Dictionary primary search (english-en-c.adf)

.....Size: 34816

.....File Version: 2000

.....Created: , Modified: 12/13/01 15:24:20

.....SHA: 6df9d2f067a411a8b72e5cbc81dbe32682b6ee44

.....MD5: b0cb1e80265b5f28fbeb97b2962d3b65



# Rainbow Tables



# Code Breaking Lookup Tables and Rainbow Table Technology

- Use pre-generated cipher text – file encryption key lookup tables to derive the key that will open 40-bit encrypted MS-Excel and MS-Word files.
- Recovery time is on the order of 1-5 minutes per file regardless of the password
- Able to provide the users login LAN and Windows NT passwords (i.e. attacking the hashes in the SAM file)

Windows



File	Type	Time	Status	Key
F:\Encrypted Files\Encrypted Word and Excel Files\balancesheet.xls	EXCEL	05:24.6	Success	d253751d8d
F:\Encrypted Files\Encrypted Word and Excel Files\Book2.xls	EXCEL	00:05.4	Success	11f274c09d
F:\Encrypted Files\Encrypted Word and Excel Files\Bypass Iomega ...	WORD	01:23.1	Success	d7e5b58ae7
F:\Encrypted Files\Encrypted Word and Excel Files\clients.doc	WORD	02:25.3	Success	c2db26beb2
F:\Encrypted Files\Encrypted Word and Excel Files\customers.doc	WORD	03:24.5	Success	7efbc9a94c
F:\Encrypted Files\Encrypted Word and Excel Files>Description.doc	WORD	02:00.2	Success	e59445d86c
F:\Encrypted Files\Encrypted Word and Excel Files\hobby.doc	WORD	00:00.3	Success	de51dc5518
F:\Encrypted Files\Encrypted Word and Excel Files\income.xls	EXCEL	00:18.7	Success	adbfc80dee
F:\Encrypted Files\Encrypted Word and Excel Files\junk.doc	WORD	00:37.3	Success	c885aa93fa
F:\Encrypted Files\Encrypted Word and Excel Files\L3tm3in2d@y4u...	WORD	02:51.4	Success	b4e3dc1c1d
F:\Encrypted Files\Encrypted Word and Excel Files\Openthepoddoo...	WORD	04:10.0	Running	
F:\Encrypted Files\Encrypted Word and Excel Files\report.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\sales.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\salesreport.xls	EXCEL		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\SaturnJupiter.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\secretplans.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\Single Space Ch...	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\Special Charact...	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\Symbol !@#.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\Symbol !@#\$\$%...	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\test.xls	EXCEL		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-2....	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-3....	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-4....	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\This is my file-5....	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\Top Row Chara...	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\Y6w2ngt5p0.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\1 space 2.doc	WORD		Queued	
F:\Encrypted Files\Encrypted Word and Excel Files\2001.doc	WORD		Queued	



# Attacking 128-bit Cryptosystems

- BestCrypt, WinZip (AES), WinRAR, PGP, DriveCrypt, etc.
- Keyspace is too large for lookup tables to be an option
- Only option is to “guess” the user’s password
- Biographical Profiling Options
  - NTUSER.DAT File
  - Web Crawling
  - FTK Export Word List
- The sweet spot for password lengths are 7-10 characters.
- The more resources that can be dedicated to the problem the higher probably of success





# Other Tools

- John the Ripper
  - Primarily a user authentication password cracker (logon)
    - Unix, Windows LAN hash
- LC5 L0phtcrack - @stake = Symantec
  - NLA



**Questions?**



# Code Breaking and Digital Forensics

FBI Supervisory Special Agent

Chris Beeson

Laboratory Director

Silicon Valley Regional Computer Forensic Laboratory

Menlo Park, CA

[cbeeson@fbi.gov](mailto:cbeeson@fbi.gov)

[www.rcfl.gov](http://www.rcfl.gov)