Windows Phone 8 Case Study: Forensic Artifacts & Challenges

Det. Cindy Murphy, MSc.
Madison Police Department
608-267-8824
cmurphy@cityofmadison.com

Detective Cindy Murphy, MSc.

- Law Enforcement Officer for 30 years
  - Madison Police Department since 1991, Detective for 15+ years
- Involved in Computer Crimes & Computer Forensics 16+ years
  - Certified Computer Forensic Examiner
  - Testified as an Expert in State and Federal Courts
  - D.F. cases in both the WI and US Supreme Court
    - US vs. Rajib Mitra – Police Radio Interference Case - 1st Prosecution of Federal Computer Crimes Statute under the Patriot Act
    - State of WI vs. Normington – Allows the use of legal pornographic images to establish motive in sexual assault cases w/ vulnerable victims
- Certified Instructor / Co-Author SANS FOR585 – Advanced Mobile Device Forensics
- MSc– University College, Dublin – Forensic Computing and Cybercrime Investigation

The Investigation…

- February 2014 @ 6:11 am- Madison, WI
- Home Invasion / Sexual Assault
- Officers Dispatched to Walgreens where victims fled after assault
  - Newly married husband and wife
  - Wife 6 months pregnant, husband legally blind
- 6 Suspects
  - 4 actively involved in the home invasion

The Investigation

- Officers respond back to residence with victims to begin investigation
- Learn that house was ransacked
  - Valuables, money, credit cards, phones taken
  - F victim later discloses multiple sexual assaults that were carried out in front of M victim
- During investigation, officers hear an altercation in the adjacent duplex unit.
  - “Feme” (prostitute, heroin addict)
  - Andy (tattoo artist, intended victim)

The Investigation

- Witness to the earlier argument says the Feme and Andy were arguing about Facebook messages.
  - Specifically a message where Feme wrote “you hit the wrong house, wtf!”
  - Says Feme was shouting, "I'm not lying!" and "They weren't supposed to bring three people."
  - Andy said he was going to show Feme's Facebook messages to the police.
  - Feme grabbed for Andy's phone and wrestled with Andy.
  - Witness helped Andy by pulling Feme away

Phone #1…

- Feme uses Andy's phone
  - Samsung SCH R950
  - Facebook and call history with family & friends
- Andy's phone was used to communicate with "Mo"
- Mo is Feme's dealer
- Feme owes Mo money
- She tells officers about Facebook messenger conversation with Mo about Andy's cash based tattoo business.

The plan…

- A plan is hatched between Feme and Mo to break into Andy's duplex to steal cash
- She says she called Mo from Andy's business and told him to call off the plan the night before
- He doesn't, and he and accomplices hit wrong half of duplex
- Feme insists she doesn't know any of Mo's accomplices, and thought that he would be alone.
- Slider door to Andy's house left unlocked by Feme.

Phone #1: Andy's Phone

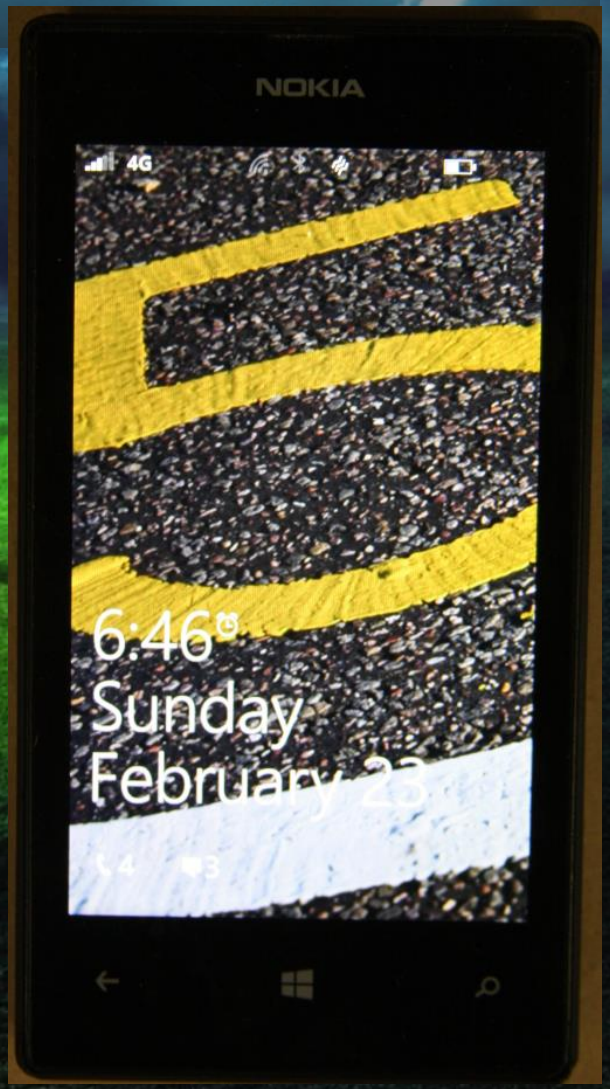
- Andy tells police he doesn't want to give up his phone
  - Claims over 1000 calls a day for 'business'
  - Officers leave phone in his custody ask him to send screen shots
- Later gives consent to download phone.
  - Done with no issues
  - Well supported by tools

Phone #2

- Every conversation has two sides…
  - Mo's phone would tie him to communications with Feme, but also could ID Accomplices
  - Mo's phone is obtained during a consent search of a GF's apartment (location found through pings of victim's phones)
  - Victim's credit cards, cash, wedding ring, and other valuables are found on his person
  - Mo arrested for Parole Violation and interviewed as a witness to the robbery
    - Cooperative for short time
    - He says he's had the phone 20 days.
    - Gives phone number
    - Wasn't asked for pass code.
  - Nokia 520 – Windows Phone 8

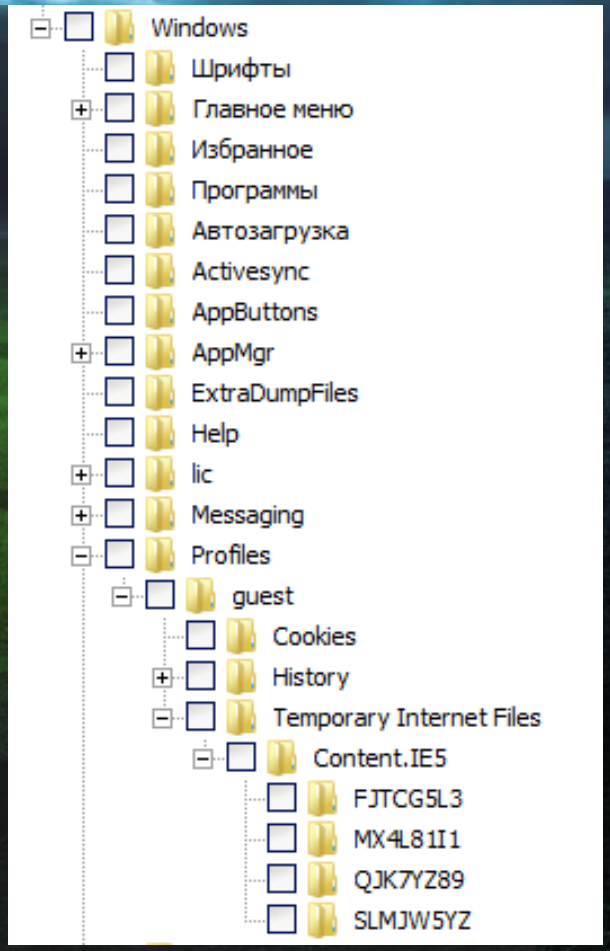
Phone #2: Mo's Phone

- Nokia 520
- Not supported for anything but logical extraction of media files via MTP
  - (At that time)
- Pass code protected
  - Unknown pass code
  - Uncooperative owner
- Demand for Speedy Trial
- Sent out for JTAG extraction



Windows Phone v. PCs

- Similarities
  - File system
  - Registry used for settings and preferences
  - Temp Files
  - Pagefile.sys
- Differences
  - Embedded (.vol) Databases
  - Registry format
  - Usage artifact and data retention

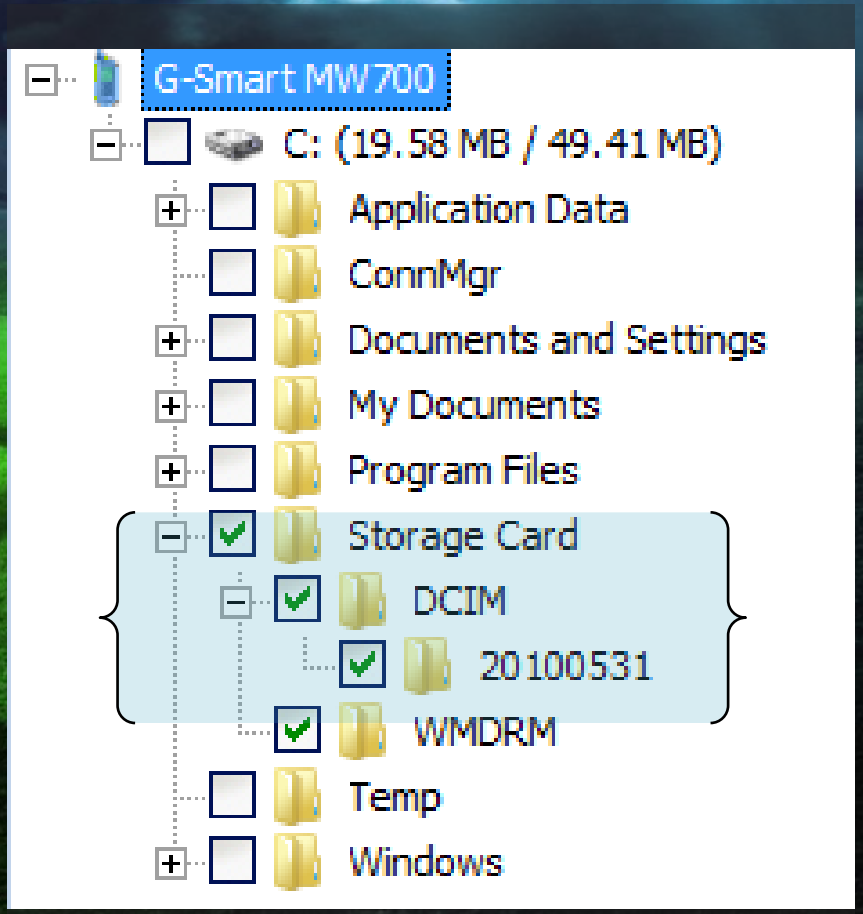


What Else is Missing?

- Windows Phone 8 / 8.1 does not use all of the same mechanisms as a Windows computer
  - No Prefetch
  - No hiberfil.sys
  - No event logs
  - No shell bags

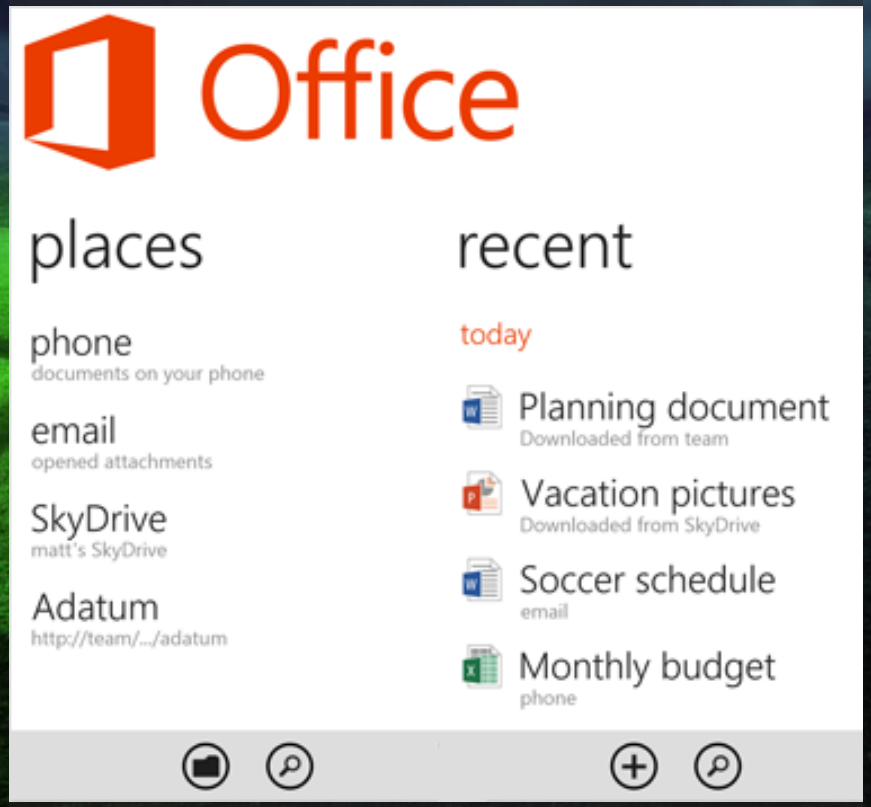
Windows Phone Removable Storage

- Windows Phone 7/8 Phones generally have a Secure Digital (SD) card slot
  - The SD card is locked to particular device with key
  - OS may automatically format newly inserted card
  - Necessary to acquire card data through the device
  - Traditional forensic tools won't read data content stored on card
  - If SD card is removed the device may not function fully



Windows Mobile Cloud Storage

- Windows 7/8 Phones are designed to sync data with the “cloud”
  - Microsoft User Accounts
    - Microsoft SkyDrive
    - Sharepoint Account
  - Data in the cloud may need to be obtained via warrant
  - Will not see cloud stored data on an RF Isolated device



Getting to the Data via USB

- **Available USB interfaces**
  - Media Transfer Protocol (MTP): music, pictures, videos, and ringtones
  - IP over USB: supports the Windows Phone SDK development tools
  - VidStream: This interface is used on retail devices to allow the phone to mirror its display to a PC.
  - KDNet over USB for debugging and interaction (registered developers only)

- **Note** If the phone is locked with a pin or if the USB data connection notification is enabled when it is connected to the PC MTP, IP over USB and VidStream don't work

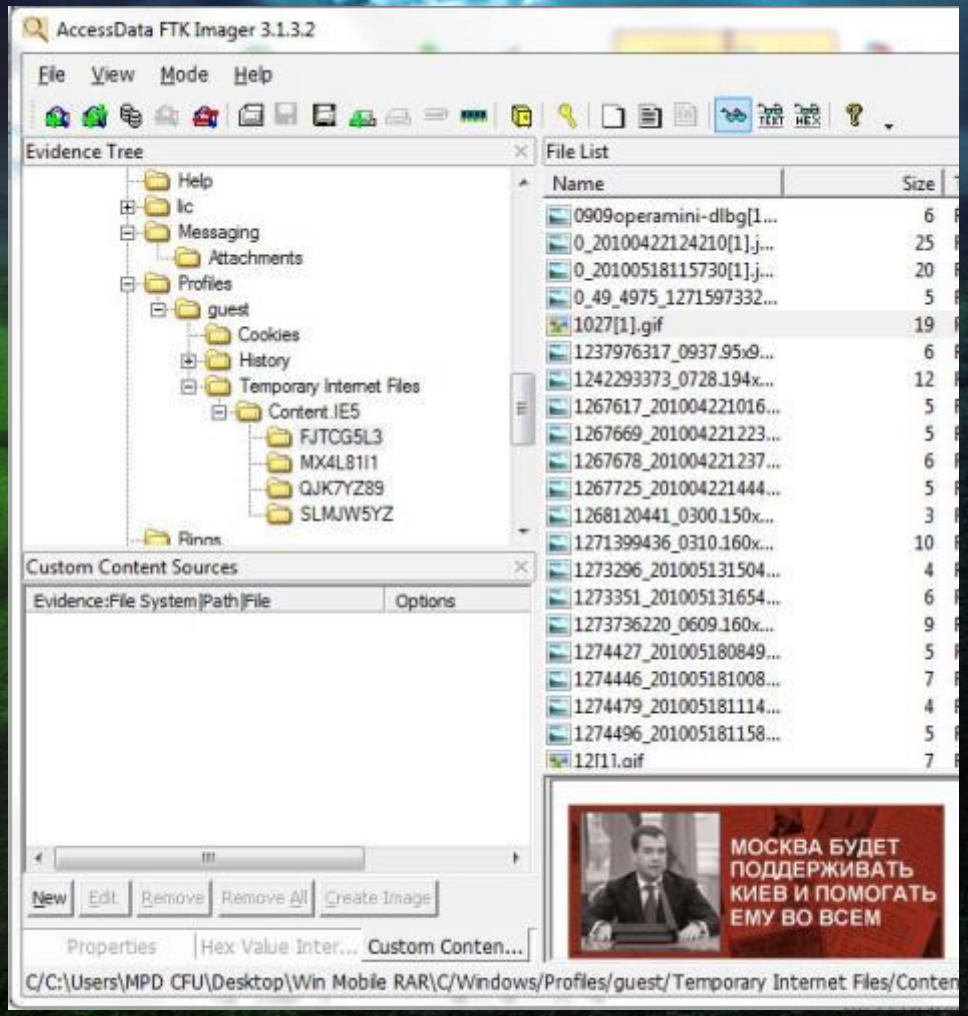
https://dev.windowsphone.com/en-us/OEM/docs/Driver_Components/USB#interfaces

Windows Mobile - PC Sync

- Windows Mobile devices are designed to be synced to a PC or Mac using the Microsoft Mobile Phone app or a variety of other methods

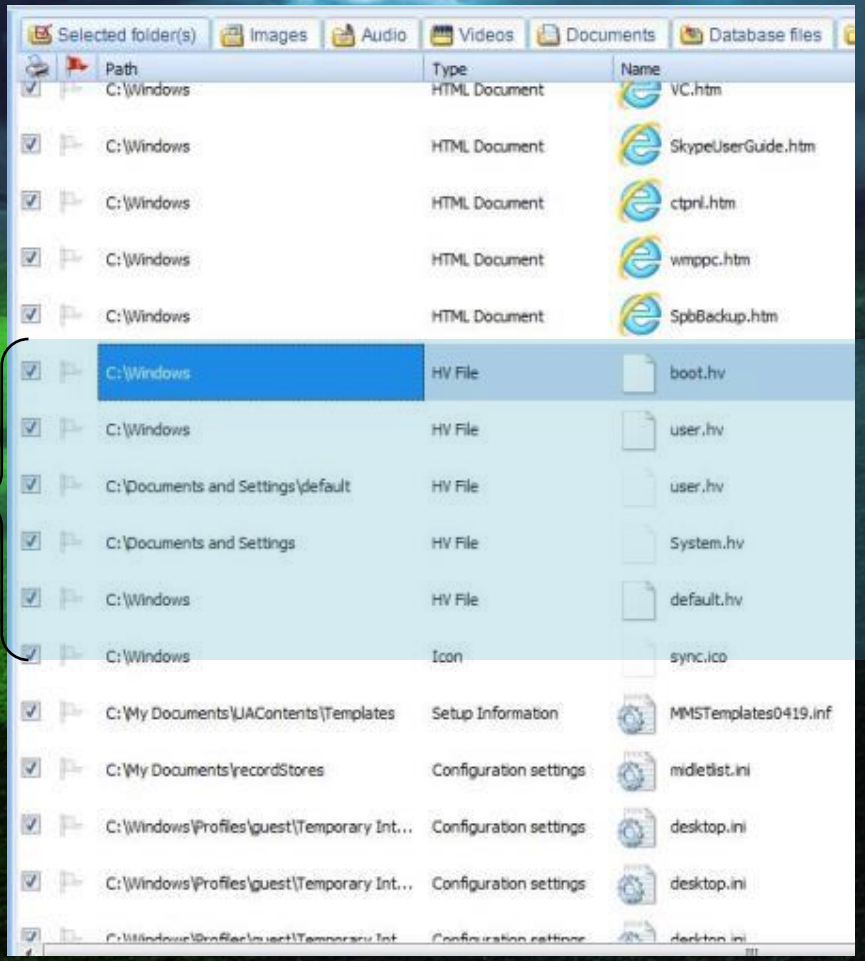
Windows Mobile Forensic Analysis

- Windows File System Forensic Tools Work!
  - EnCase 7
  - X-Ways
  - FTK
- Varying levels of support by mobile forensic tools
  - Generally not so good… but improving.



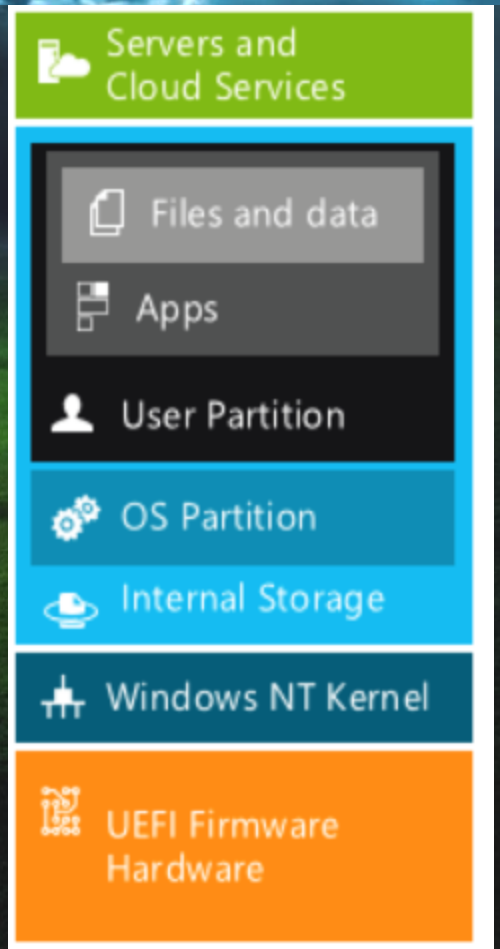
Windows Mobile Registry Analysis

- Stored in hive files
  - Active registry files are locked by operating system
  - Prevents copying
- Read by some tools
  - Presented in XML format
- Remote Registry Editor



Windows Phone 8 Security

- Windows Phone 8 uses Trusted Boot and code signing to ensure integrity
  - Protects against malware and rootkits
  - Only validated software components can execute
- Trusted Boot validates firmware images before they are allowed to load the OS
- ALL binaries must be signed by a trusted authority
- System-on-a-Chip (SoC) also used in addition, pre-boot



Layered security platform diagram

Windows Phone 8 Encryption

- Bitlocker Technology is used for encryption of all internal data
  - AES 128
- Once enabled, phone automatically begins encrypting internal storage
- Encryption key protected by Trust Platform Module (TPM)
- Combined PIN and Bitlocker make data very secure

Windows Phone 8

- Windows Phone 8 supports use of extended memory via Micro SD
  - Only allows storage of media files
    - Pictures, movies, music
  - Access to stored data via MTP
- Windows Phone OS and user data partitions are* encrypted, files stored on Micro SD are not
- Wipe of Device can be initiated remotely or locally by the user
- If incorrect PIN is entered too many times, local wipe is initiated

Windows Phone 7/8 Forensics Acquisition Support

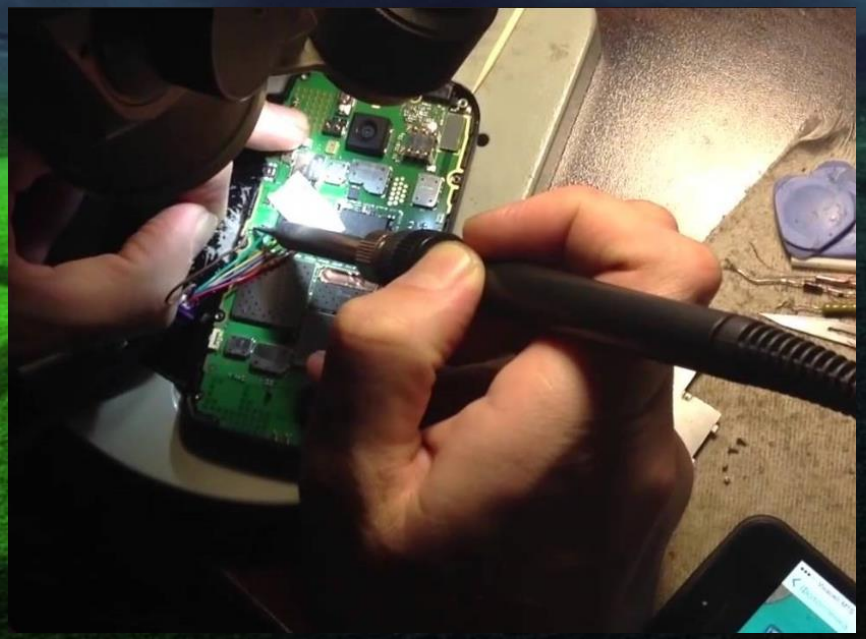
Logical	File System	Physical

• Limited support available for most forensic tools
• Images, Video, Sounds – from external storage
• Contact List
• Call Logs
	• Very limited support by some forensic tools
	  • Cellebrite
	  • XRY
	  • Oxygen
	• May only acquire file system of external storage device
		• JTAG or chip off only
		• Cellebrite supports some devices
		• Forensic tools may support decoding & limited parsing of the raw extraction
		  • XRY
		  • Cellebrite
		  • Oxygen
		  • EnCase 7
		  • X-Ways

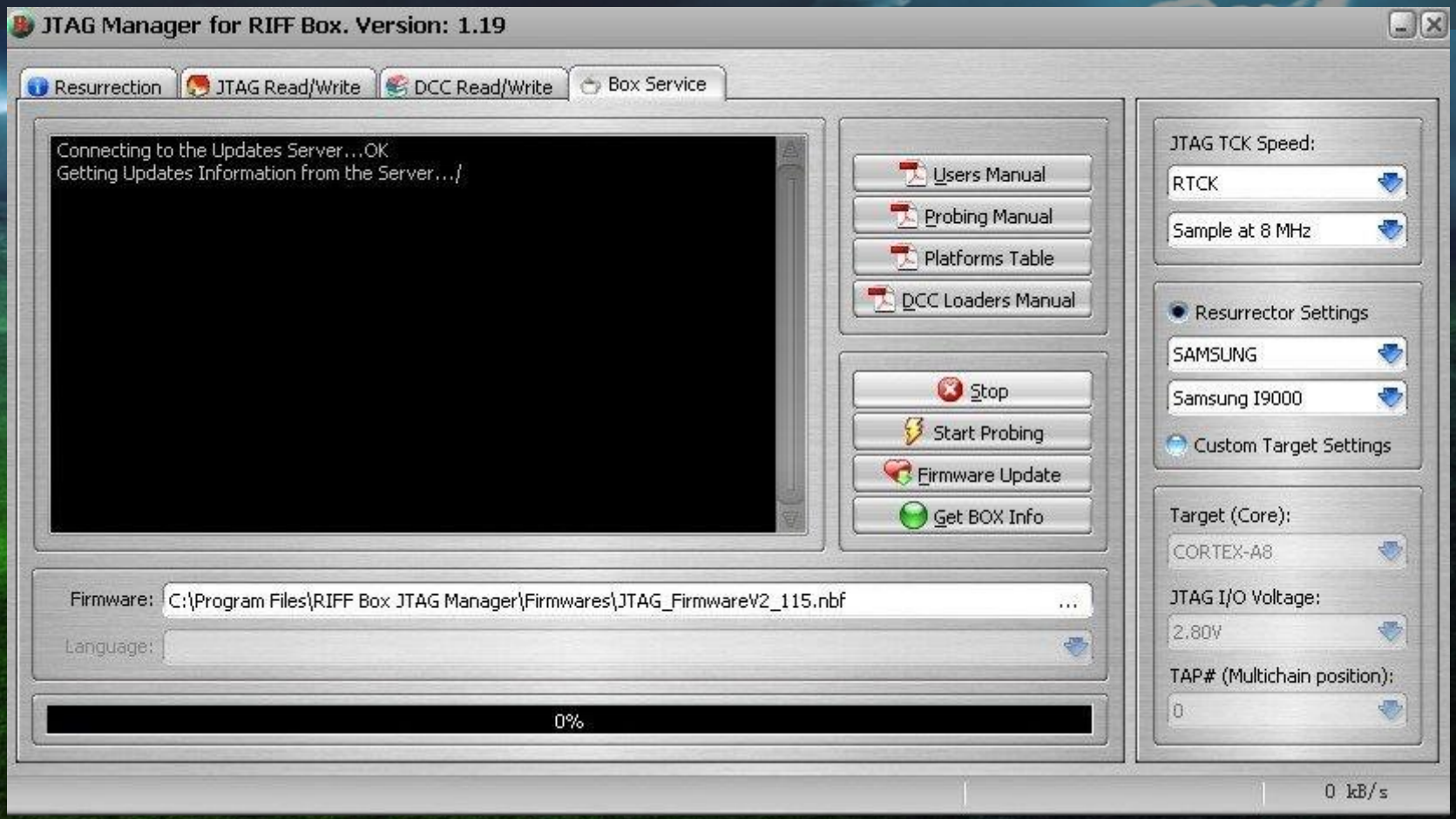
JTAG Extraction

JTAG Extraction

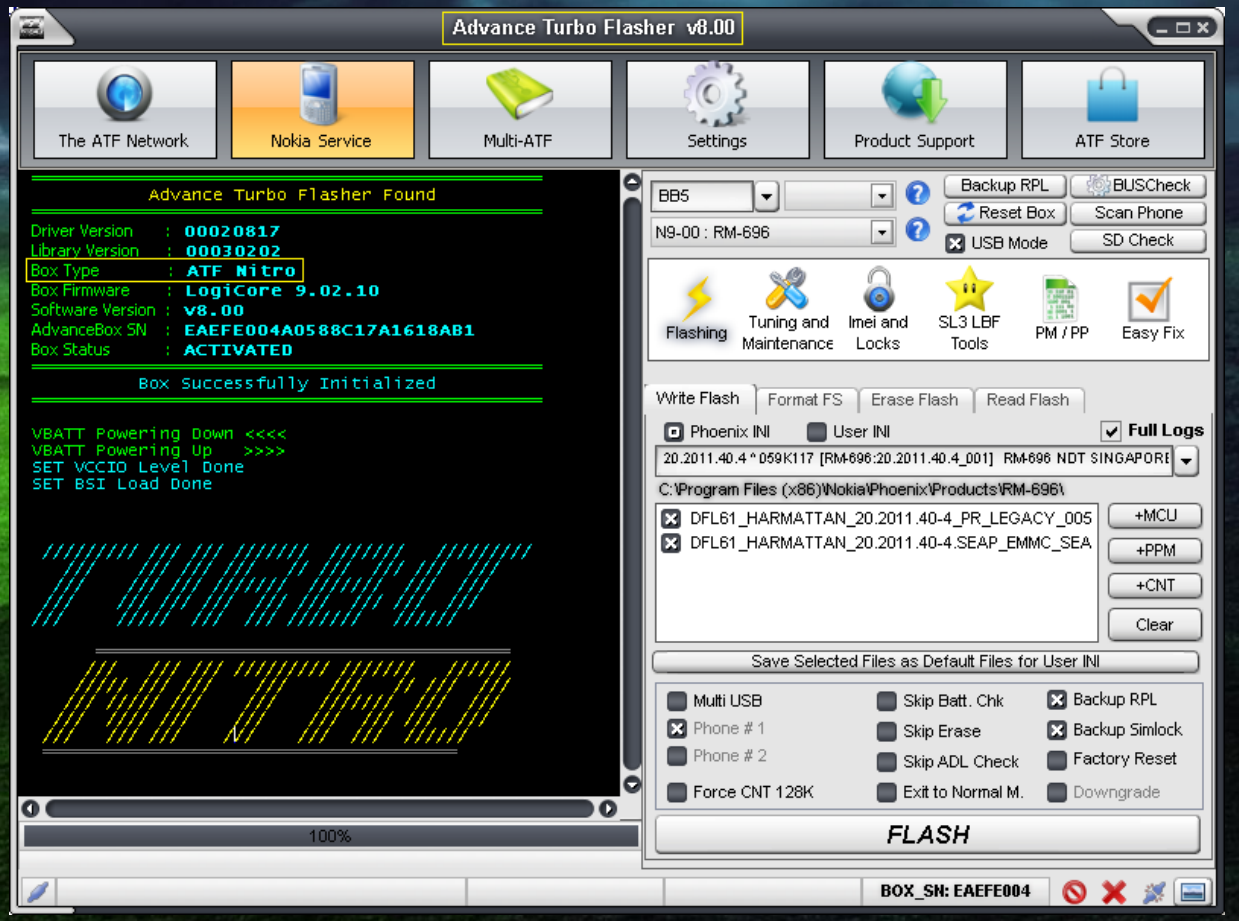
- RIFF Box
- ATF Box
- Quick Example of JTAG setup:
  - https://www.youtube.com/watch?v=VyBC0DrkmMk
- Many boxes / jigs / adapters
  - all support different phones
  - Teel Tech provides great kits and training!



RIFF Box



ATF Box



Working with the Extraction:

- Raw .bin file is returned
  - Contains full physical image of memory from chip
  - Forensic tools may or may not parse the file system
- In this case, Cellebrite didn't parse File System
- X-Ways Did.
- EnCase 7 Did.
- TEAMWORK!!

Use Multiple Tools

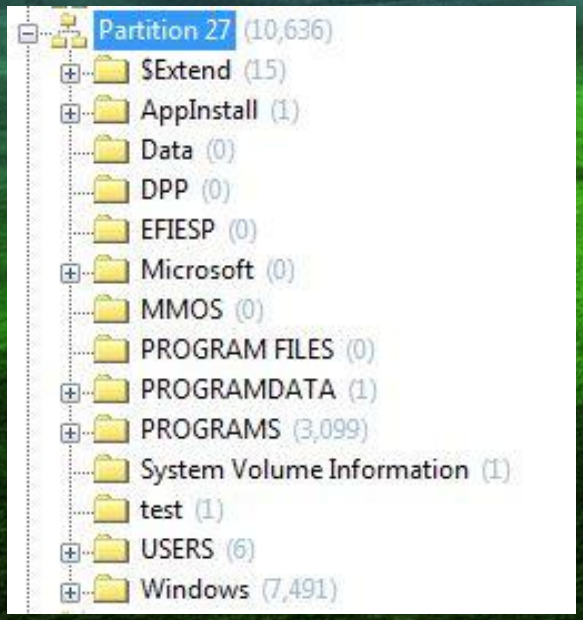
- For most extensive visibility of data
  - EnCase
  - X-Ways
  - Cellebrite
  - IEF
  - Database viewers
  - Python Scripting
- Dive in and dig.
  - Keywords
  - Find and parse dates

Narrowing the Focus

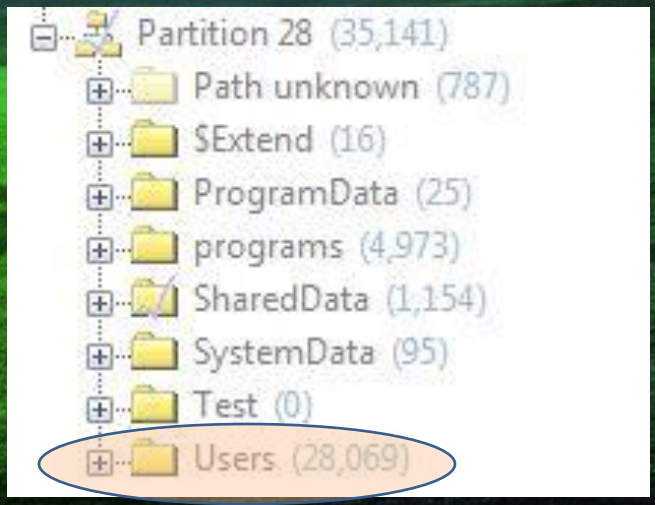
- Partition 27 and 28 were imported into Cellebrite Physical Analyzer to leverage
  - Scripting tools
  - Bookmarking
  - Mobile centric date / time / data decoding tools

28 Partitions?

System Data



User Data



28,069 Users??

Windows Phone 8 User Accounts

- There are actually 25 default user accounts
  - Tool interpretation of data can be misleading
  - Most user accounts used by the OS for services
- Three Important User Accounts to focus on:
  - Public
  - WPCOMMSSERVICES
  - DEFAPPS

User: Public

- Contains multimedia files:
  - Documents, Music, Pictures, Ringtones, Videos
  - This part of the file system is accessible when the phone is connected to a Windows PC.
  - Pictures folder:

    - "Camera Roll" subfolder contains photos taken with the internal camera

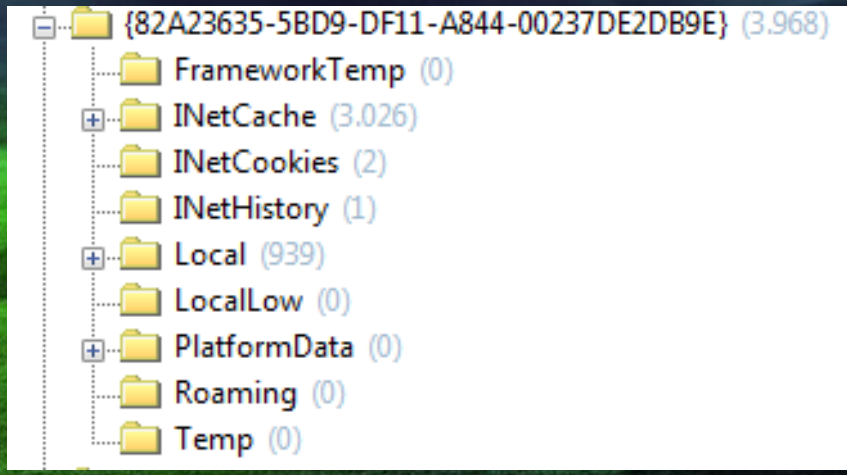
    - "Saved Pictures" subfolder contains photos saved from applications (ex. Facebook)

    - "Screenshots" subfolder contains phone monitor screenshots

    - "WhatsApp" subfolder contains WhatsApp pictures (if installed, of course)

User: DEFAPPS

- Contains data from applications
  - preinstalled and third party
- Preinstalled Apps have their own folders
- Every third party application is identified by an App ID
- The internal structure of every application folder is consistent
- Application related data (database and config) stored in the subfolder **Local**
- Cache data is stored in the **INetCache** folder
- Cookies are stored in the **INetCookies** folder



User: WPCOMMSSERVICE

- Store.vol
  - Phone base features
  - SMS, Email, MMS, attachments
  - Contacts information (table has 131 columns!)
- Phone
  - Call logs
- These are ESE database files, but they aren't standard
  - "xEF xCD xAB x89" present at bytes 4-8

- Method:
  - String searches
    - Phone numbers
    - Text
    - UTF-16 Encoding used
  - Date Time Format
    - 8 byte MS FILETIME stamps
- Tools:
  - FTK shows tables well
  - OSForensics
  - ESE Database viewer

Phone database format

- **Phone** database contains call history inside **Call History** table
  - Important fields:

Type (0 = Outgoing Call; 1 = Incoming Call; 2 = Missed Call)
Raw Number
Raw CallerID
Resolved Contact
Start Time
End Time

*Start and End times are in FileTime format (100-nannoseconds sincs Jan 1 1601)

Store.vol database format

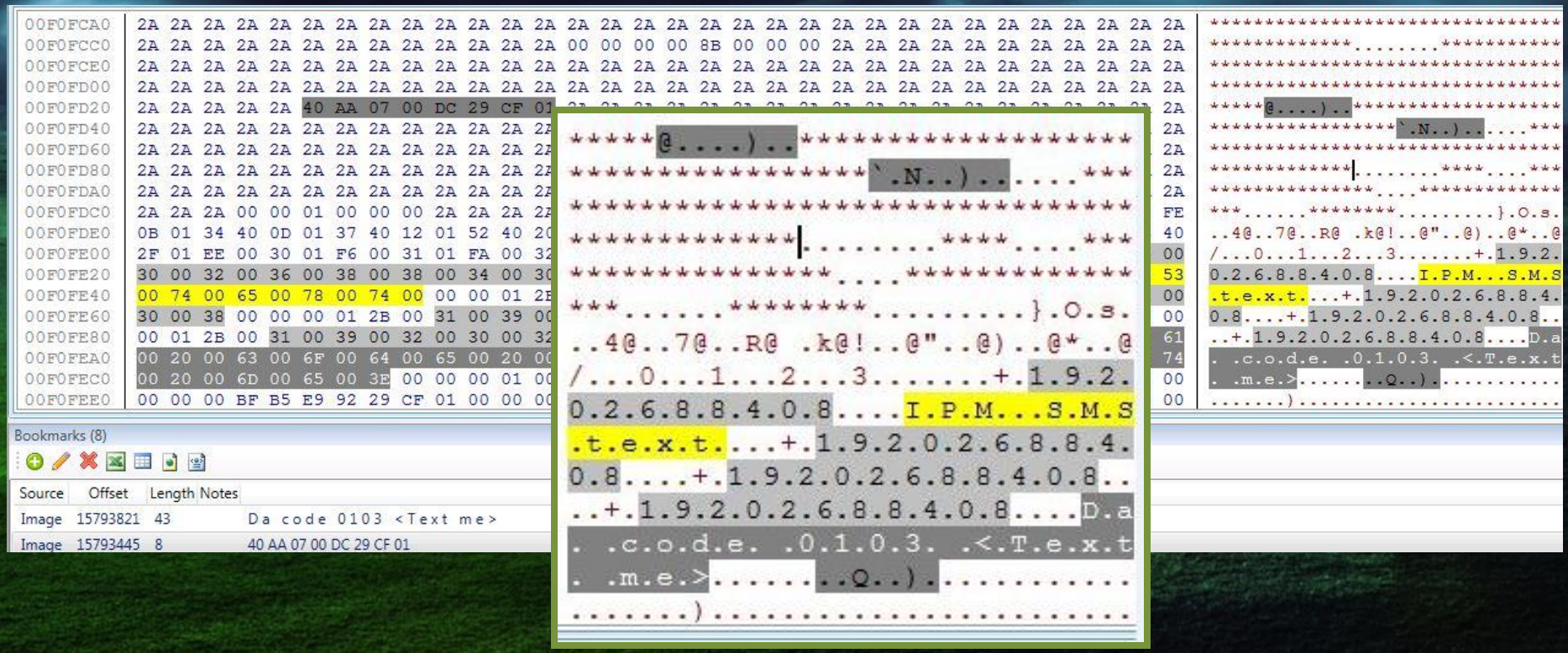
- **Message table (SMS Message)**

  Type (1 = Received; 33 = Sent)
  Label
  IPM.SMSText
  IPM.MMSText
  Text
  Date and time (FileTime format)

- **Appointment Table**

  Start Time (FileTime)
  Duration (minutes)
  Type (all day, appointment)
  Text
  Place

Sometimes you get lucky…



The code actually was 0103…!

Patterns… and Variations

- SMS Messages
  - Sent SMS have no telephone number stored in record
  - Received SMS messages contain phone number
- Flags for message status
- Distance in bytes between date/time stamp and message

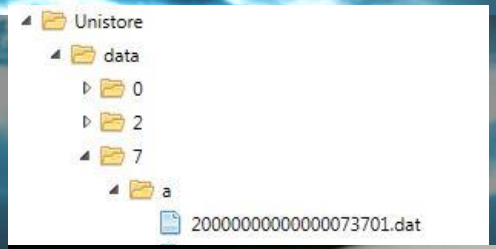
Python Scipts

Windows Phone 8.0 SMS, Call History and Contacts Scripts

Apparently, you can't trust any old monkey with your Windows Phone ...

- http://cheeky4n6monkey.blogspot.com/2014/10/windows-phone-80-sms-call-history-and.html

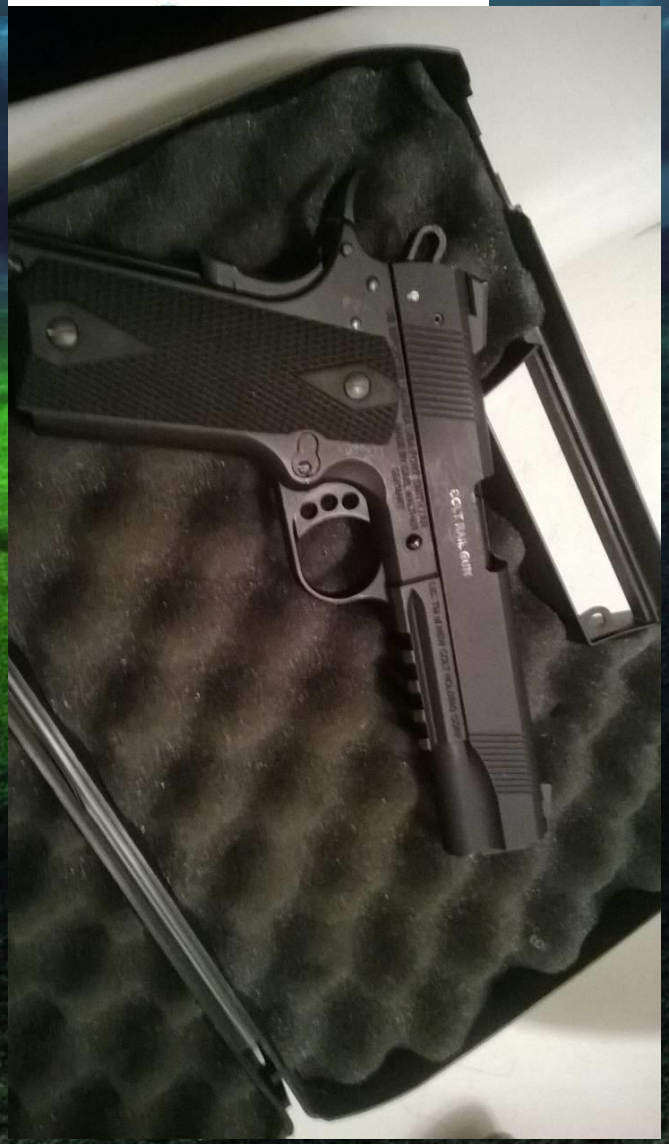
MMS Messages

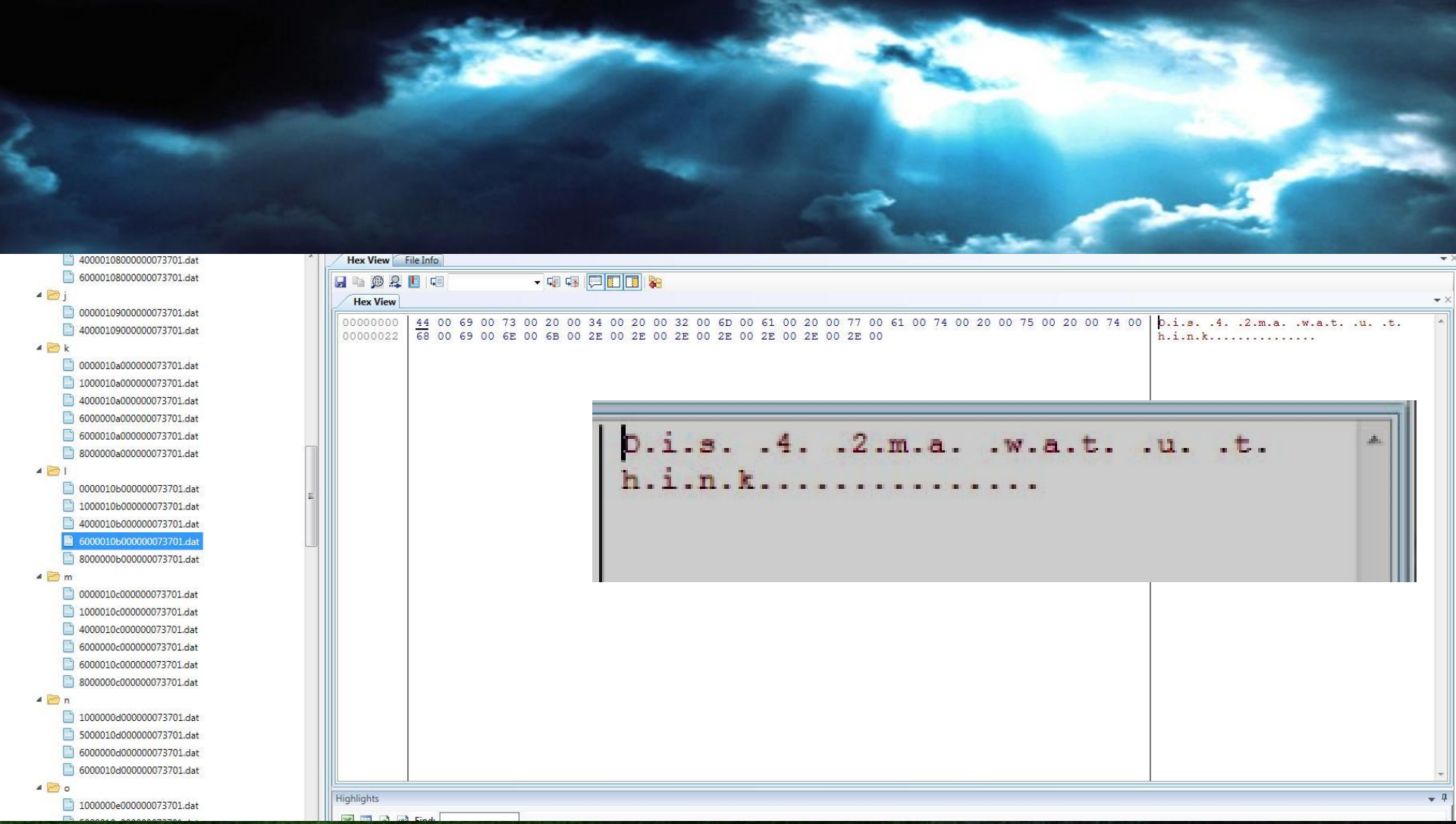


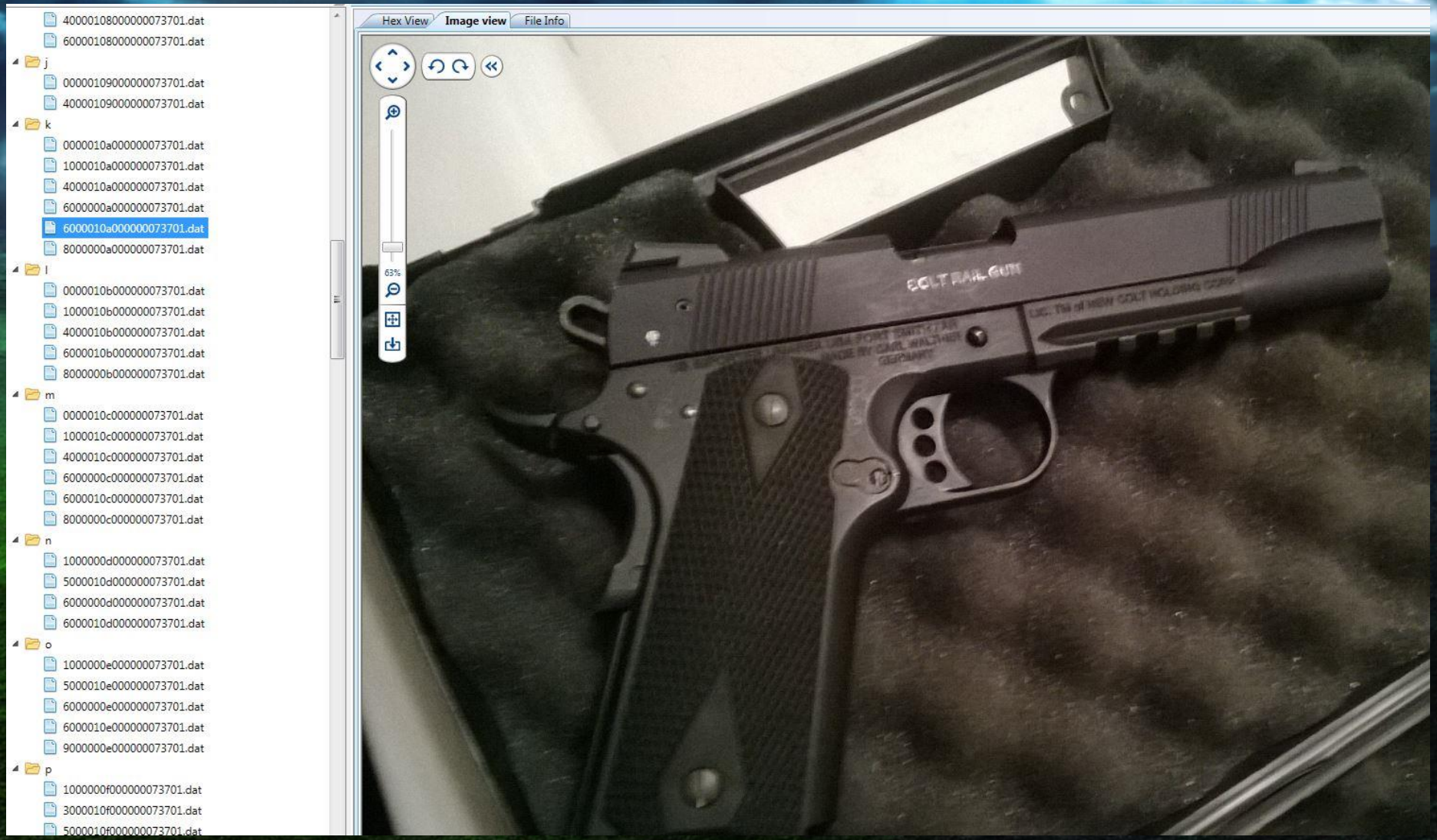
- **Record of message itself:**

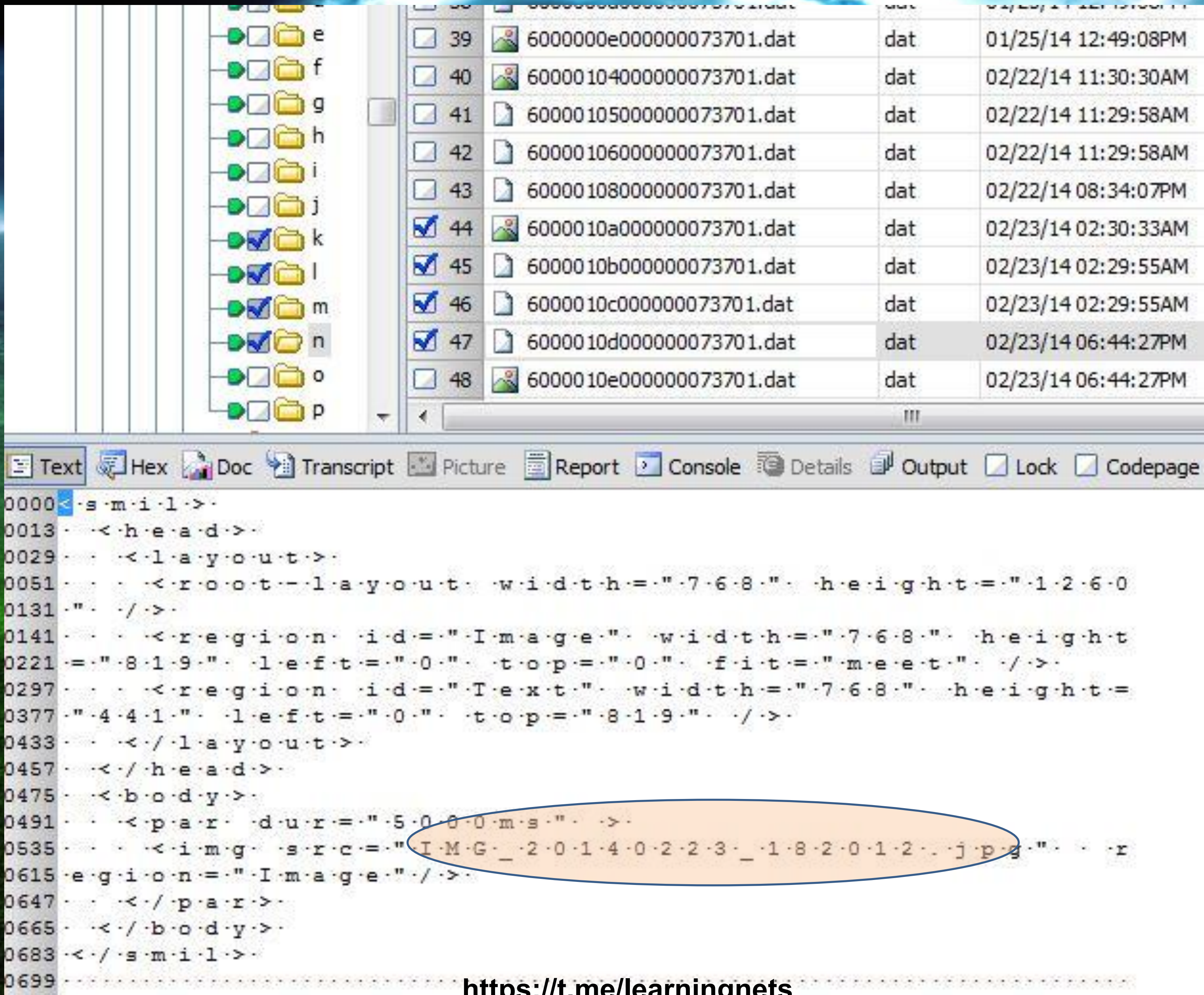
  \Users\WPCOMMSSERVICES\APPDATA\Local\Unistore\store.vol

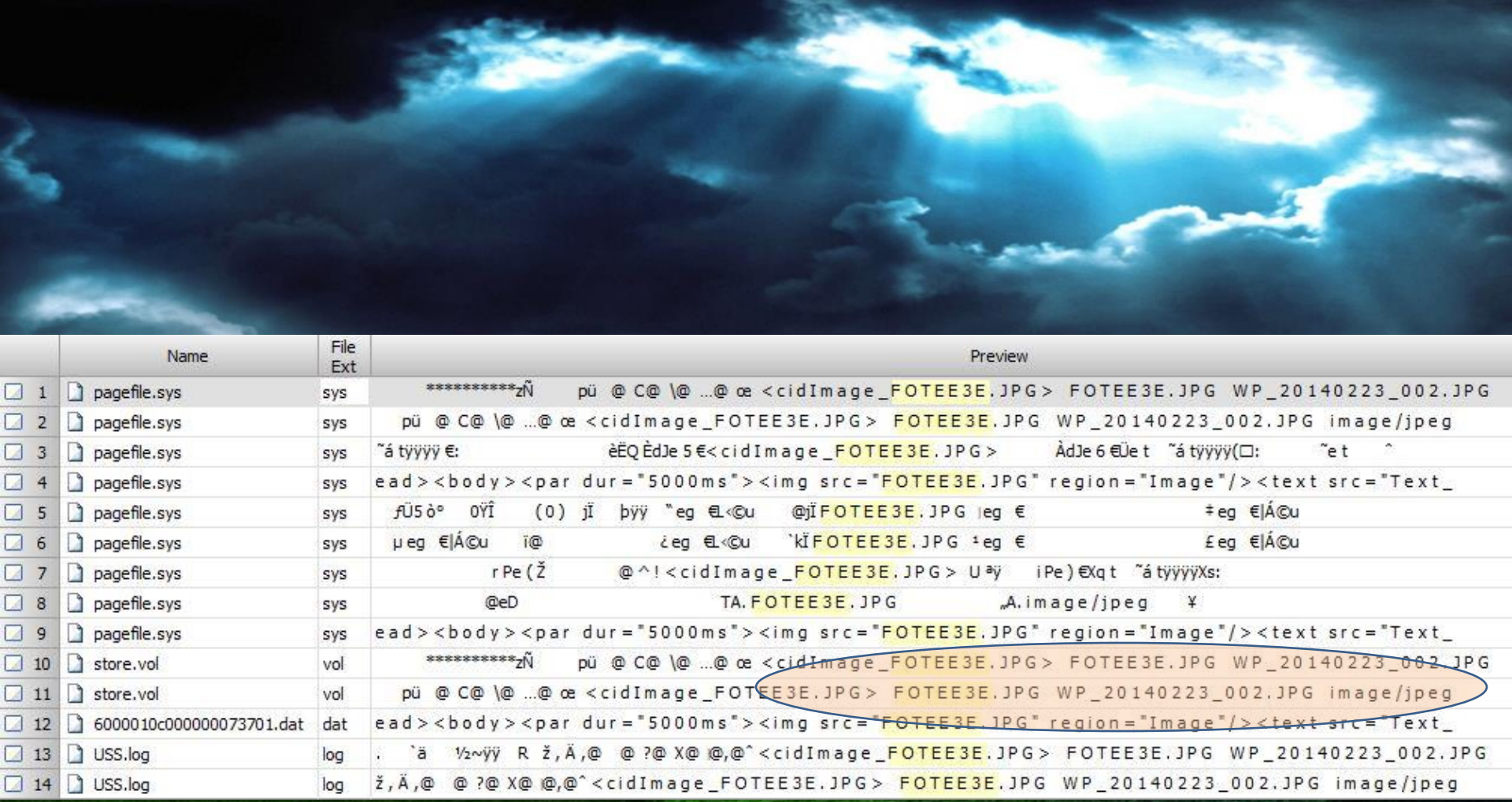
- Content, attachments and formatting info are stored in .dat files
  - **SharedData\Comms\Unistore\data**
- Multiple .dat files for individual messages
  - Naming convention?? Ugh.
- 3 sub-directories:
  - "0", "2" and "7”
  - Appear to correspond to Draft, Received and Sent











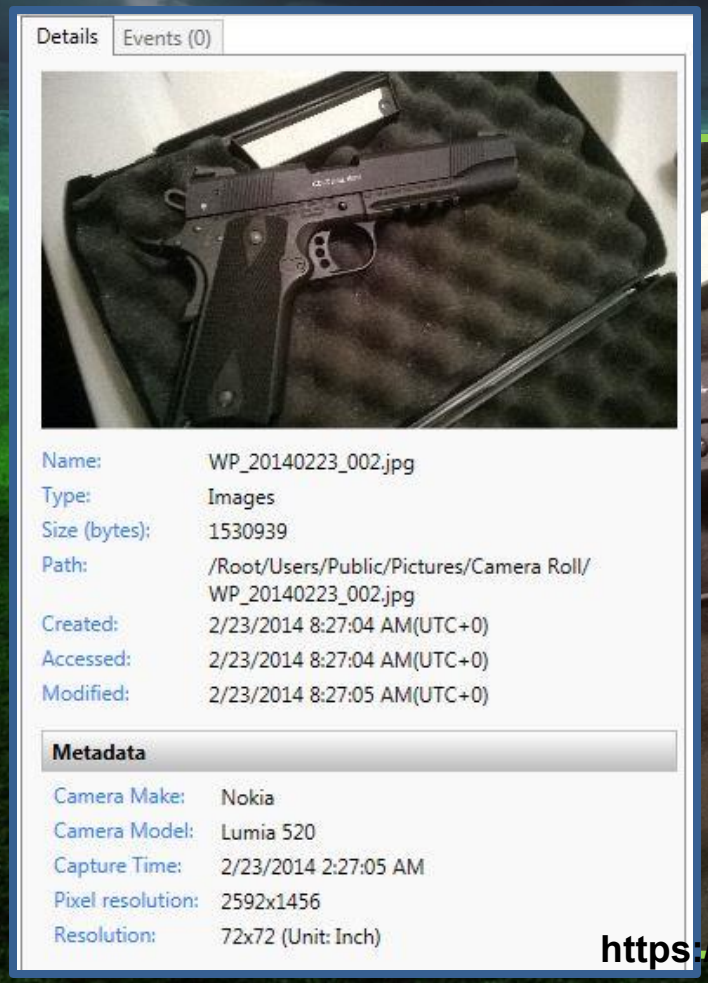
	Name	File Ext	Preview
1	pagefile.sys	sys	**********zÑ pü @ C@ \@ …@ œ <cidImage_FOTEE3E.JPG> FOTEE3E.JPG WP_20140223_002.JPG
2	pagefile.sys	sys	pü @ C@ \@ …@ œ <cidImage_FOTEE3E.JPG> FOTEE3E.JPG WP_20140223_002.JPG image/jpeg
3	pagefile.sys	sys	˜á tÿÿÿÿ €: èËQ ÈdJe 5 €<cidImage_FOTEE3E.JPG> ÀdJe 6 €Ùe t ˜á tÿÿÿÿ(□: ˜e t ^
4	pagefile.sys	sys	ead><body><par dur="5000ms"><text src="Text_
5	pagefile.sys	sys	ƒÜ5ò° 0ŸÎ (0) jÏ þÿÿ "eg €L‹©u @jÏFOTEE3E.JPG ¦eg € ‡eg €¦Á©u
6	pagefile.sys	sys	µeg €¦Á©u ï@ ¿eg €L‹©u `kÏFOTEE3E.JPG ¹eg € £eg €¦Á©u
7	pagefile.sys	sys	rPe(Ž @^!<cidImage_FOTEE3E.JPG> Uªÿ iPe)€Xqt ˜á tÿÿÿÿXs:
8	pagefile.sys	sys	@eD TA.FOTEE3E.JPG „A.image/jpeg ¥
9	pagefile.sys	sys	ead><body><par dur="5000ms"><text src="Text_
10	store.vol	vol	**********zÑ pü @ C@ \@ …@ œ <cidImage_FOTEE3E.JPG> FOTEE3E.JPG WP_20140223_002.JPG
11	store.vol	vol	pü @ C@ \@ …@ œ <cidImage_FOTEE3E.JPG> FOTEE3E.JPG WP_20140223_002.JPG image/jpeg
12	6000010c000000073701.dat	dat	ead><body><par dur="5000ms"><text src="Text_
13	USS.log	log	. `ä ½~ÿÿ R ž,Ä,@ @ ?@ X@ @,@^<cidImage_FOTEE3E.JPG> FOTEE3E.JPG WP_20140223_002.JPG
14	USS.log	log	ž,Ä,@ @ ?@ X@ @,@^<cidImage_FOTEE3E.JPG> FOTEE3E.JPG WP_20140223_002.JPG image/jpeg

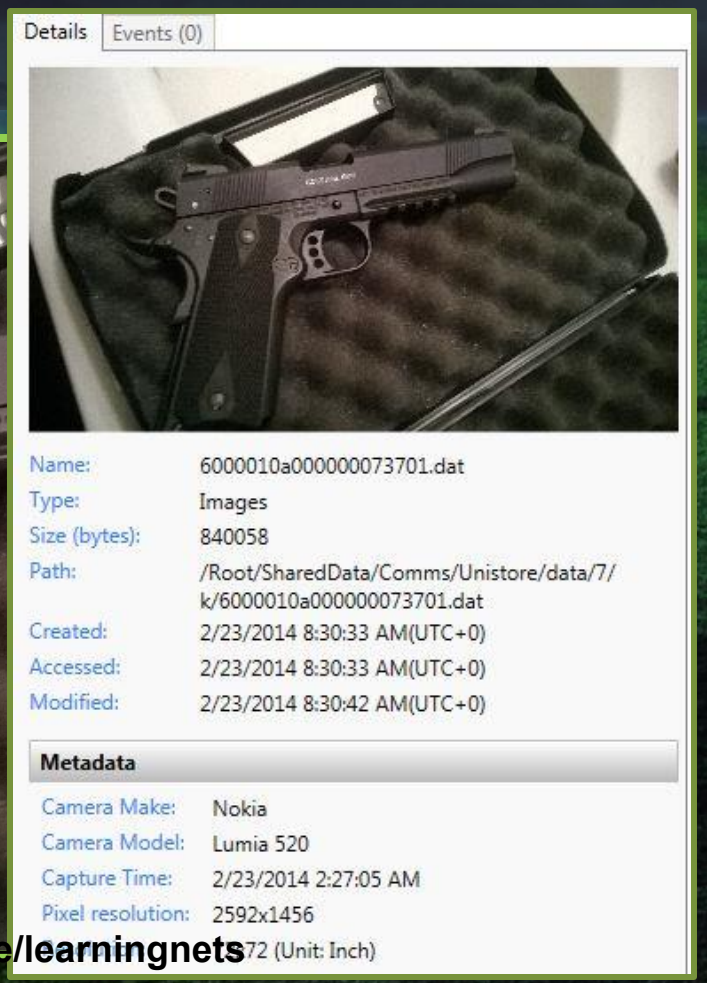
Date & Time Stamps

- For this make and model of phone, the timestamp wasn't displayed with the message.
- We got more from the underlying data than the screen

Images and Videos

- Users/Public/Pictures/CameraRoll/ WP_YYYYMMDD_###.jpg





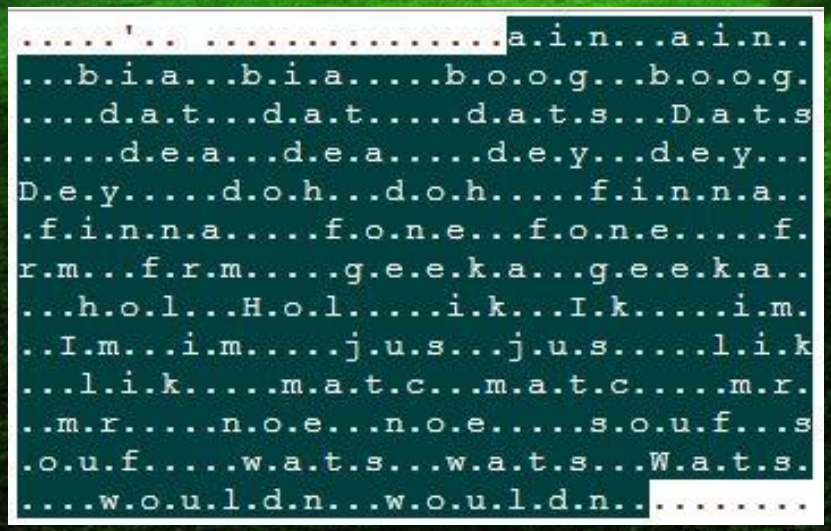
Video File

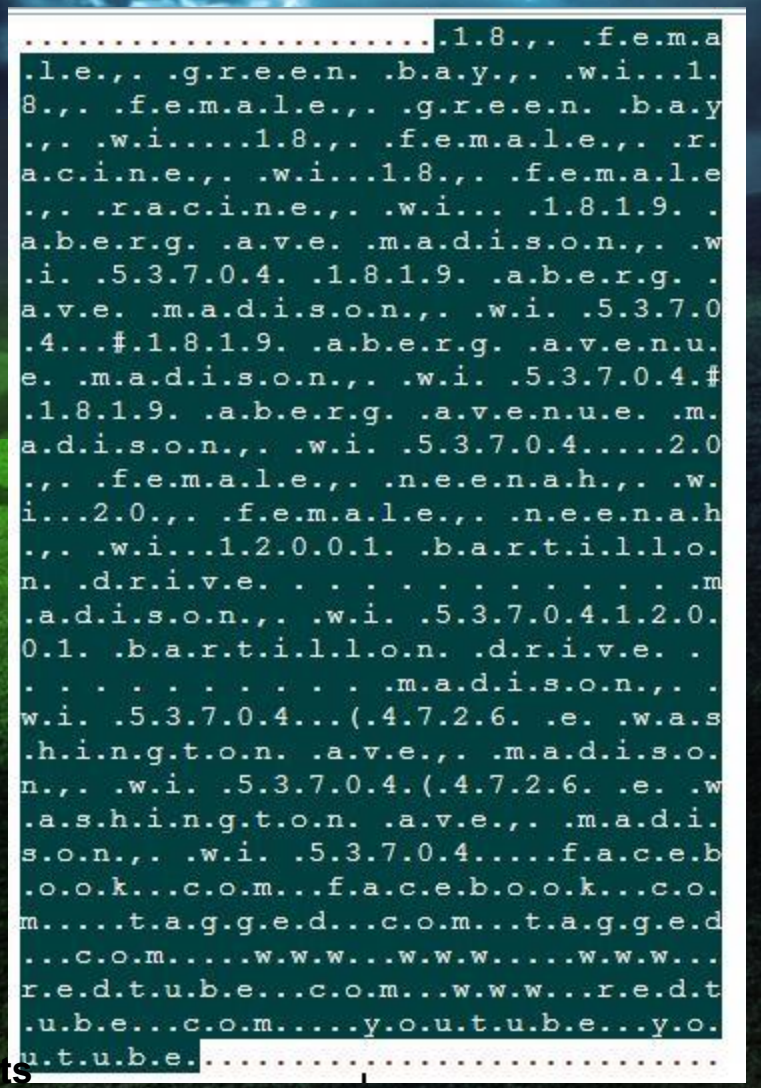
Thumbnail Index Images

- **Users/Public/Pictures/CameraRoll/ WP_YYYYMMDD_###.mp4**

User Dictionaries…
(my current favorite artifact)

- SharedData/Input/neutral/
  - livehds.dat – form history
  - ihds.dat – user input words





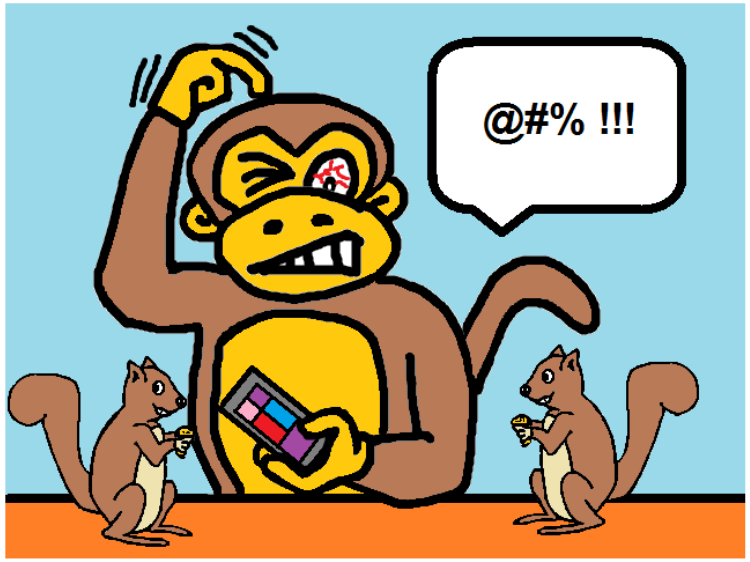
Windows 8 Phone Artifact locations

File or Location	Description
Users/WPCOMMSERVICES/APPDATA/Local/Unistore/Store.vol	SMS Contacts
Users/WPCOMMSERVICES/APPDATA/Local/UserData/Phone	Call History
Users/DefApps/APPDATA/INERNETEXPLORER/INetCache/	Internet browsing history Cookies
Users/Public/Pictures/CameraRoll/ WP_YYYYMMDD_###.jpg	Pictures taken with the device Videos taken with the device
Users/Public/Pictures/SavedPictures/	Pictures saved to the device from other sources (Facebook, etc...)
Users/WPCOMMSERVICES/APPDATA/Temp/RequestManager/Cache	Cached images from message attachments
SharedData/Comms/Messaging/Temp/MMS	File attachments from incoming and outgoing mms messages
SharedData/Comms/Unistore/Data (in various subfolders)	MMS Attachments MMS Formatting Information MMS Message Content
SharedData/Input/neutral/	ihds.dat - user input word list livehds.dat – form history

Leveraging the DF/IR Community

Friday, 13 June 2014

Monkeying around with Windows Phone 8.0



Ah, the wonders of Windows Phone 8.0 ... Failing eyesight, Frustration and Squirrel chasing

$LogFile		29,696 KB
$MFT		44,544 KB
$UsnJrnl:$J		209,308 KB

DEFAULT		2/9/2014 9:22 PM
NTUSER.DAT		3/7/2014 2:52 AM
SAM		2/9/2014 9:22 PM
SECURITY		2/9/2014 9:22 PM
SOFTWARE		2/9/2014 9:22 PM
SYSTEM		2/9/2014 9:22 PM

pagefile.sys	3/4/2014 10:26 PM	System file	262,144 KB
USS.chk	3/4/2014 10:26 PM	Recovered File Fra...	8 KB
USS.log	3/4/2014 10:26 PM	Text Document	3,072 KB
USS00024.log	2/22/2014 6:00 PM	Text Document	3,072 KB
USSres00001.jrs	3/6/2013 3:27 AM	JRS File	3,072 KB
USSres00002.jrs	3/6/2013 3:27 AM	JRS File	3,072 KB
USStmp.log	2/21/2014 3:30 AM	Text Document	3,072 KB

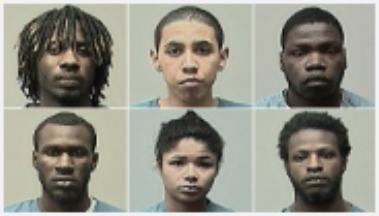
Thanks to…

- Adrian Leong – Cheeky4n6monkey
- Maggie Gaffney – Teel Tech
- JoAnn Gibb – Ohio Attorney General's Office
- Brian McGarry – An Garda Siochana
- Shafik Punja – Calgary Police Service
- Ron Serber, Ronen Engler, etc… - Cellebrite
- Mattia Epifani – REALITY NET System Solutions
- Francesco Picasso - REALITY NET System Solutions

The End Result …

MADISON, Wis. -The last of the six people involved in a violent home invasion on Madison's east side at the end of February was sentenced Tuesday.

RELATED CONTENT



Top: Eric Bass, Kristopher Hughes, Demarco Mallit Bottom: Deandrae Mayweathers, Efemia Neumaier, and Michon Thomas. Bass, Hughes, and Thomas faces sexual assault charges.

Pedestrian dies after being hit by car at East Wash, Stoughton Road intersection

McFarland firefighters battle residential blaze

Minister gets 30 years for sexual assaults in Green Bay area

DeForest man suffers serious injuries in crash between pickup-moped crash

Kristopher Hughes, 20, was sentenced to 15 years in prison and 10 years of supervised release for two counts of armed robbery. Hughes pleaded guilty to the charges on July 25.

The three charges of first-degree sexual assault were dismissed, but were read in to the sentencing.

The incident, in which a pregnant woman was sexually assaulted, happened on Quincy Avenue around 4 a.m. on Feb. 23, according to a release. Madison police called the incident a "violent home invasion."

The victims had guns pointed at their head and heard the robbers say "someone is gonna die tonight," according to a criminal complaint. During the robbery, the men took electronics, credit and debit cards, and jewelry.

The three men were initially planning on robbing a man who Efemia Neumaier was staying with, but accidentally broke into the home of the victims, according to the complaint. Neumaier planned the robbery with one of the men, saying the man she was staying with would have a lot of cash the night of the robbery.

DeAndrae Mayweathers Jr., 23, was previously sentenced to 14 years in prison and 8 years supervised release on two counts of armed robbery.

Michon A. Thomas, 23, was sentenced to 25 years in prison and 20 years of supervised release on two counts of armed robbery and three counts of first-degree sexual assault.

Eric Bass, 24, was sentenced 25 years in prison and 15 years of supervised release on two counts of armed robbery and three counts of first-degree sexual assault.

Demarco D Mallit, 23, was sentenced in August to two years in prison and two years of supervised release. He was charged with theft and aiding a felon.

Efemia Neumaier, was sentenced in September to five years in prison and five years of extended supervision. She was charged with robbery with the use of force.

Questions?
Comments?
Suggestions?