



v6.5

Présentation CNEJITA
Jean Louis Courteaud Juin 2013

XRY v6.5

Plus de 9000 appareils supportés

V6.5 Les Nouveautés

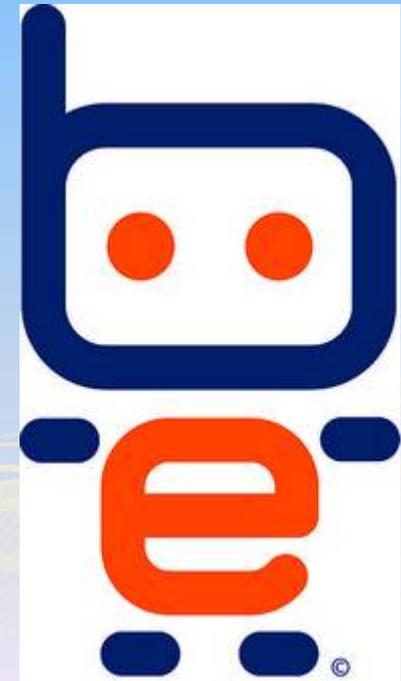


- ✓ Extraction plus rapide
- ✓ BlackBerry Physical Decoding
- ✓ Amelioration des Dump sous Android 4.0
- ✓ Extraction Iphone en mode Recovery
- ✓ Nouvelles applications Smartphones

Extractions Simultanées



Nouvelles applications



XRY vs UFED

- **Avant tout « Complémentaires »**

 Vitesse d'extraction + Extractions simultanées

Reader gratuit et diffusable

Extractions simultanées

Hot Line

Fonctionne sur tout support Windows (Tablette)



– Editeur Hexadécimal peu performant

PRIX PUBLIC XRY

Logical 3500 Euros HT + 1500 Euros HT/an

**Physical 7000 Euros HT + 3200 Euros
HT/an**

XAMN



C'est quoi

- Une solution logicielle permettant l'analyse et le recoupement du contenu de plusieurs téléphones (25+10).
 - Outil désigné spécifiquement pour les investigations téléphoniques.
 - Import direct des fichiers XRY et CELLEBRITE
 - Visualisation des différentes connexions (téléphones, SMS, MMS, chats, contacts,...)
 - Utilisation des géodatas.
 - Filtres différents.
- 

Pourquoi?

- De plus en plus de données à traiter ... et à recouper.
- Pratiquement toutes les dossiers mettent en jeu plusieurs téléphones.
- Savoir faire en examen de téléphones = Pratique standard, la nouveauté c'est le volume.

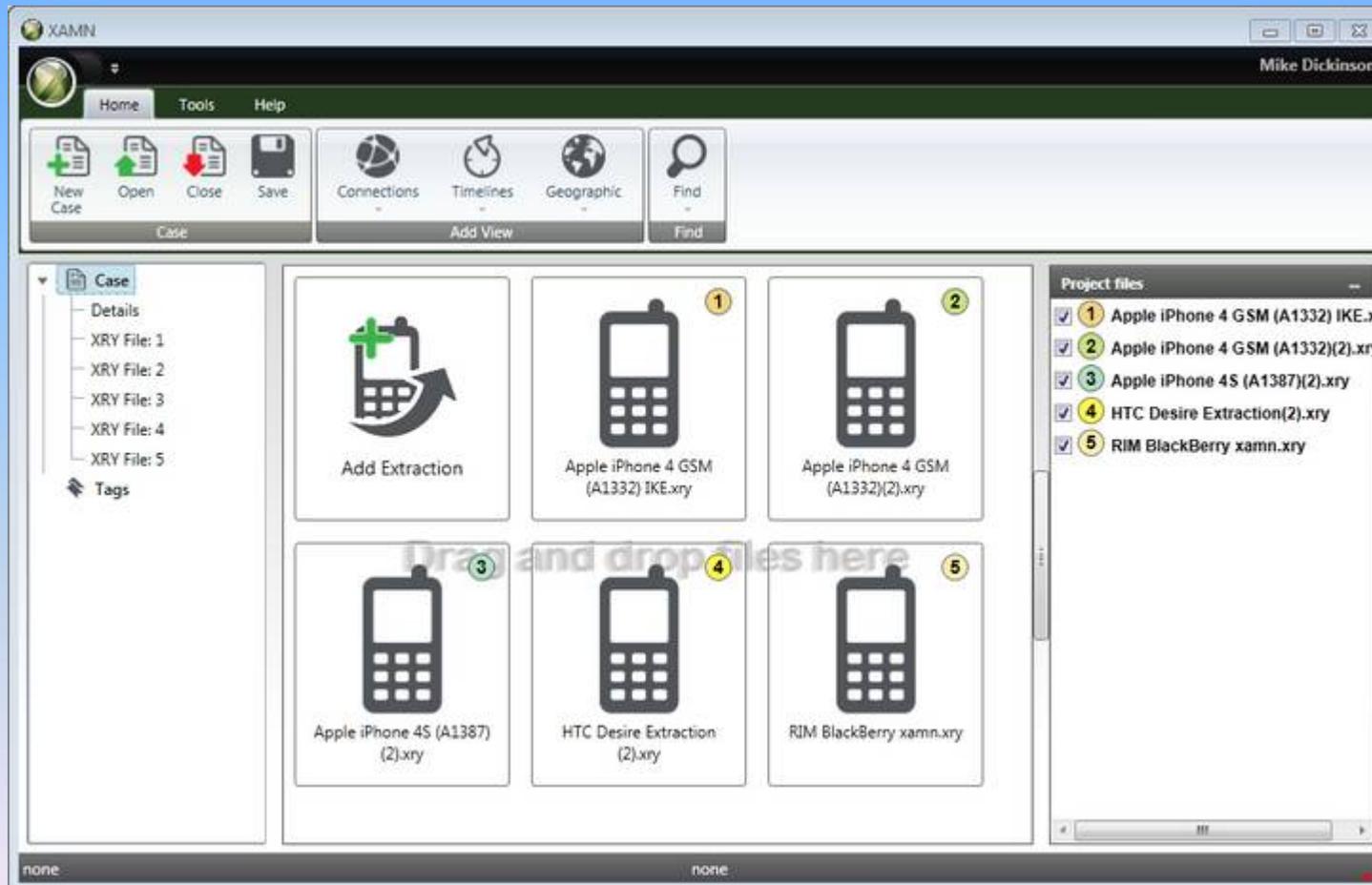
Périmètre

1. Visualiser les liens, horodatage.
2. Appréhender les gros volumes de données.
3. Comparer et rechercher différents profils entre eux.
4. Comprendre le volume d'information à analyser.
5. Présenter les résultats sous forme de schémas simples.

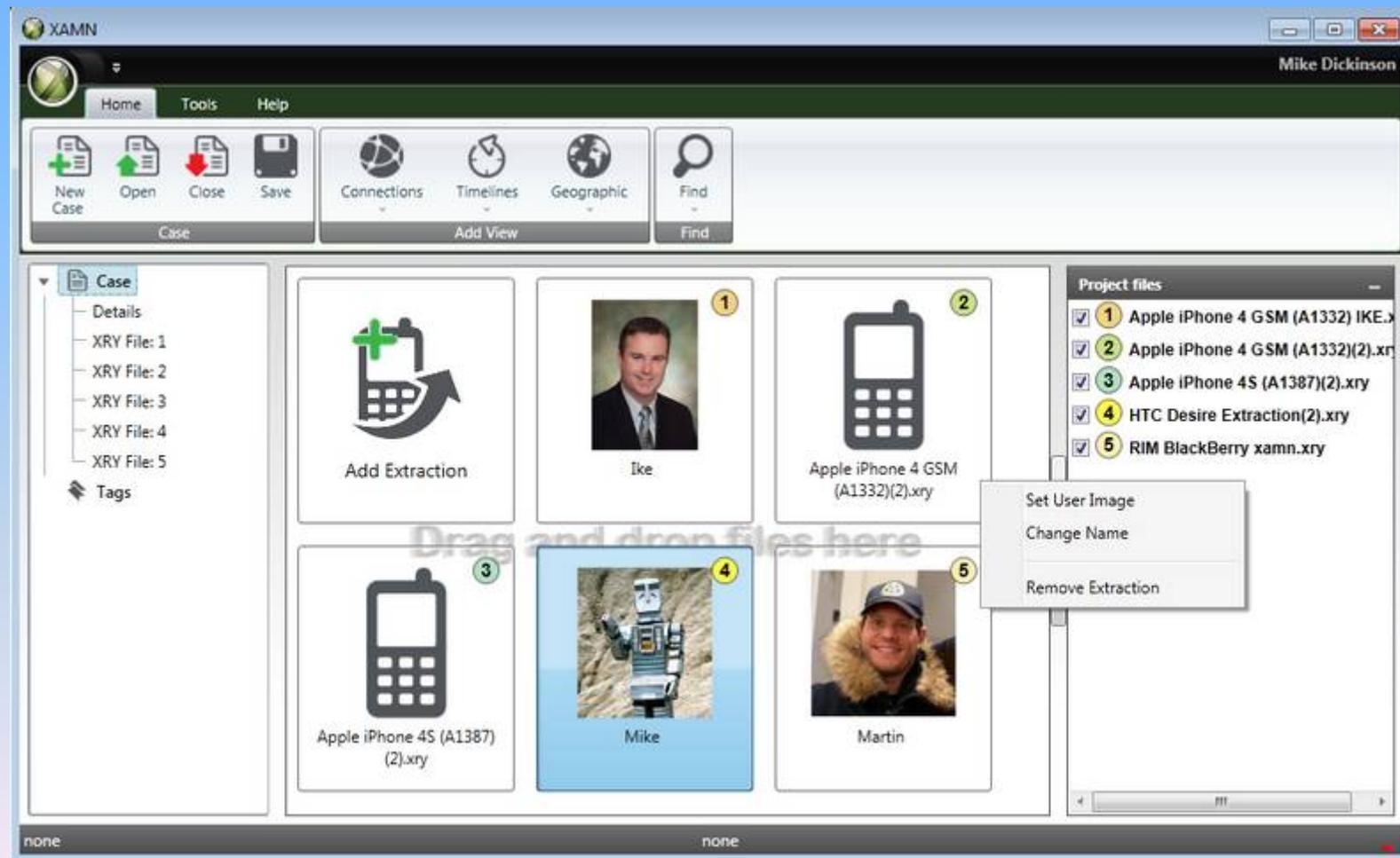
Cible

- Utilisateurs XRY.
- Analystes et investigateurs.
- Equipes internes de sécurité.
- Forces de l'ordre.
- Services de renseignements.

Drag & Drop Fichiers XRY



Personnalisation des appareils



Appréhension du volume global



Résumé de chaque fichier

The screenshot displays the XAMN software interface. The main window title is "XAMN" and the user is "Mike Dickinson". The interface is divided into several sections:

- Case Details (Left Pane):** Lists "XRY File: 1" through "XRY File: 5" and "Tags".
- Main Summary (Center):** Displays details for "C:\Users\mick\Dropbox\XAMN Training\Apple iPhone 4 GSM (A1332) iKE.xry".
 - Display Name:** Apple iPhone 4 GSM (A1332) iKE.xry
 - Owner Name:** Apple iPhone 4 GSM (A1332) iKE.xry
 - Owner Phone:** 1
- Image: Logical**
 - Date Created:** 30/08/2012 13:06:17
 - Locked:** No
 - Extraction Media:** iPhone
 - XRY Version:** 6.3.1
 - Is File Subset:** Yes
 - Subset Created:** 30/08/2012 13:55:42
 - Is Encrypted:** No
 - Case Reference:** 12-00058
 - Exhibit Id:** 1A
 - Case Operator:** John Doe
 - Notes:**
 - Crime:** 187 PC
 - Owner:** Ina Victim
- Summary Legend:**
 - Contacts [3 items]
 - Calls [3 items]
 - Messages/SMS [6 items]
 - Messages/MMS [1 items]
 - Messages/Chat [2 items]
 - Files/Pictures [3 items]
- Message Log (Right Window):** Shows a list of messages with columns for Number, Name, and Name.

Number	Name	Name
+4670011515	Mike Dickinson	Mike Dickinson
+44 7833 439065	Shaun Sutcliffe	Shaun Sutcliffe
+44 7833 439065	Shaun Sutcliffe	Shaun Sutcliffe
+447833439065	Shaun Sutcliffe	Shaun Sutcliffe
+46740511515	Mike Dickinson	Mike Dickinson
+46 78-051 15 15	Mike Dickinson	Mike Dickinson

Voir les connexions

The screenshot displays the XAMN software interface. The main window shows a network diagram with various nodes representing mobile devices and a central contact. A pop-up window titled "3 Connection data" is open over one of the nodes, displaying the following information:

Name #0	Mike Dickinson
Name #1	The Guv
Numbers #0	+46760511515
📞 Calls	0
📇 Contacts	1
📧 Messages	12

The interface also includes a menu bar (Home, Tools, Help), a toolbar with icons for New Case, Open, Close, Save, Connections, Timelines, Geographic, and Find, and a sidebar with a tree view showing Case details and Connections. On the right, there are panels for Project files and Filters.

Project files:

- 1 Apple iPhone 4 GSM (A1332) IKE.xry
- 2 Apple iPhone 4 GSM (A1332)(2).xry
- 3 Apple iPhone 4S (A1387)(2).xry
- 4 HTC Desire Extraction(2).xry
- 5 RIM BlackBerry xamn.xry

Filters:

- [Calls] Number 5
- [Calls] Call time
- [Calls] Call length
- [Contacts] Name
- [Contacts] Nickname
- [Contacts] Number
- [Messages] Content
- [Messages] Number 5

Affichage et visualisation des Timelines

The screenshot displays the XAMN software interface, which is used for analyzing mobile communication data. The main window shows a timeline visualization of events, with a detailed view of a specific event selected.

Interface Elements:

- Menu:** Home, Tools, Help
- Toolbar:** New Case, Open, Close, Save, Connections, Timelines, Geographic, Find
- Left Panel:** Case (Details, XRY File 1-5), Tags, Connections (All), TimeLine (All)
- Main Timeline:** A horizontal timeline showing events from 2009 to 2012. The selected event is a call on 2012/06/29 at 06:49:07.
- Bottom Panel:** Project files and Details.

Project files:

- 1 Apple iPhone 4 GSM (A1332) IKE.xry
- 2 Apple iPhone 4 GSM (A1332)(2).xry
- 3 Apple iPhone 4S (A1387)(2).xry

Details:

[2012/06/29 06:49:07] XRY File ID: 1 XRY Category: MMS	
Name	Shaun Sutcliffe
Name	Shaun Sutcliffe
Index	4743
Date	29/06/2012 06:49:07 UTC (Default)

Visualisation des Géotags

The screenshot displays the XAMN software interface. The window title is "XAMN" and the user name is "Mike Dickinson". The interface includes a menu bar (Home, Tools, Help) and a toolbar with icons for "New Case", "Open", "Close", "Save", "Connections", "Timelines", "Geographic", and "Find".

The main area shows a map of Europe with three geotags highlighted in yellow boxes:

- Tag 1: 2012/07/17 (2) - located in the Republic of Ireland.
- Tag 2: 2012/07/16 (4) - located in the Baltic region (Eesti).
- Tag 3: 2012/07/17 (2) - located in Germany (Deutschland).

The left sidebar shows a tree view with the following structure:

- Case
 - Details
 - XRY File: 1
 - XRY File: 2
 - XRY File: 3
 - XRY File: 4
 - XRY File: 5
- Tags
- Connections
 - All
- TimeLine
 - All
- Geographic
 - GeoMap

The bottom panel shows a list of project files and their details:

Project files	Details
<input checked="" type="checkbox"/> 1 Apple iPhone 4 GSM (A1332) IKE.xry	[2012/07/17 15:02:24] XRY File ID: 2 XRY Category: Locations/Bookmarks
<input checked="" type="checkbox"/> 2 Apple iPhone 4 GSM (A1332)(2).xry	Application: Navfree GPS Live iphone.gbl
	Misc: Home

The status bar at the bottom indicates "none".

A améliorer

- Restitution automatique sous forme de reports graphiques et exploitables.



Résumé

- Complément à XRY ... Et à Cellebrite
- Permet de mieux appréhender l'information.
- Meilleure explication des causes et des faits.
- Spécialement conçu pour les téléphones.
- Recherche multifichiers de données.
- Visualisation des liens, contacts, connectés directement ou non.

PRIX PUBLIC XAMN

- Licence 2 500 Euros HT
- Redevance annuelle 900 Euros HT.