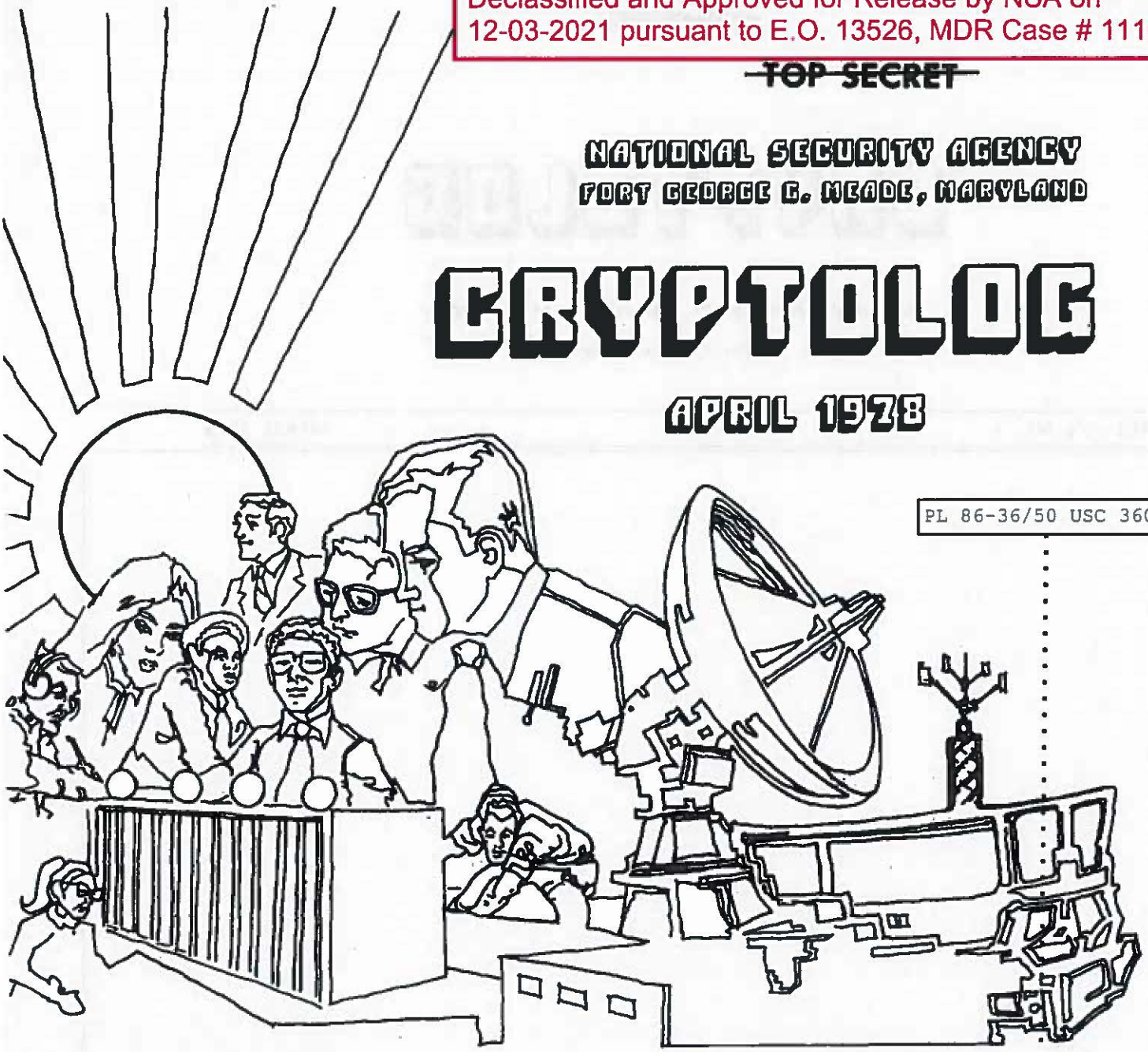
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1978



PL 86-36/50 USC 3605

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)
Exempt from GDS, EO 11652, Category 2
Declassify Upon Notification by the Originator~~

Non - Responsive

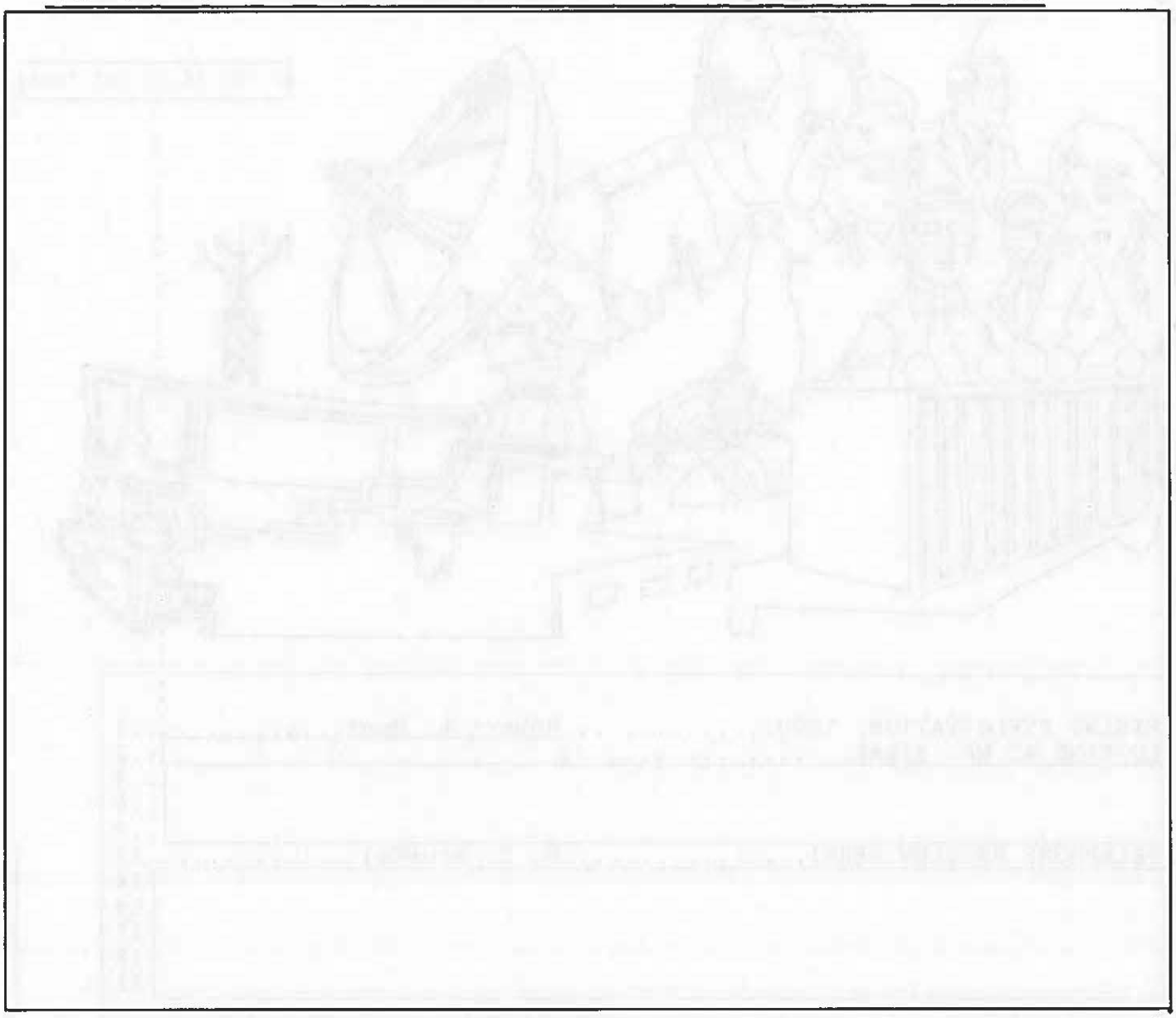
~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

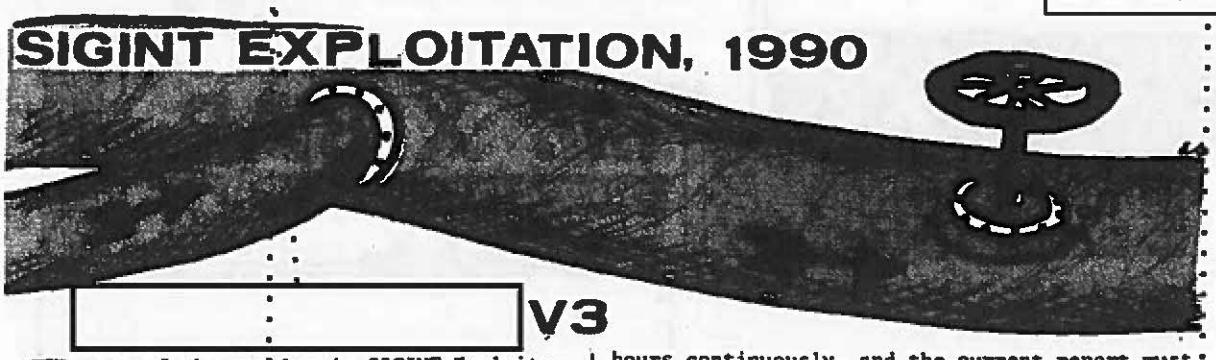
VOL. V, NO. 4 APRIL 1978



~~TOP SECRET~~

Non - Responsive

SIGINT EXPLOITATION, 1990



[redacted] V3

Part of the problem in SIGINT Exploitation for the 1980s and 1990s is the simultaneous increase in collection capacity because of improved technological sophistication, and the decrease in analytic and reporting capability because of fiscal restraints. To put it simply, we are collecting more and exploiting less. There is a crying need to master the technology (which constantly threatens to drive our collection) and apply it smartly to assist our analysis and exploitation. If we cannot manipulate the massive amounts of data we are now able to collect, we are reduced to the primary function of selecting the constipation point in the SIGINT system. Do we inundate our collection facilities and arbitrarily cut off the incoming data in order to alleviate the load at the processing point? Do we allow free flow of voluminous collection to deluge the processors and confine our processing to artificially stringent limits, gambling that what is missed will not be missed? Or, do we overwhelm our customers with profuse and indigestible amounts of [redacted] gambling that what is significant will be summarized?

What alternatives are there to preselecting the blockage area? We must master our machines for use in analysis, processing, and reporting as well as in collection, so that the monster that gathers also sifts. While we cannot eliminate the human element in exploitation, we must provide help to that human element -- the individual hers and hims -- in massaging the huge pile of material we are funneling into the SIGINT system. We must also gear the mechanical wizards we are building and buying to aid our reporters in preparing and presenting the information gleaned for specific customers who need it, in a timely and lucid manner. We must also design the machines to be used so that the human drivers can operate quickly, comfortably, and efficiently. This concept is more complex than it appears since it encompasses both human-engineering aspects like, "Can the terminal be operated with existing lighting by someone wearing bifocals?", and mechanical aspects like, "Can the operator get a report out in minutes to the right customers in a crisis when the computer system is saturated, the terminal has been operating for 72 hours continuously, and the current report must take precedence over 48 others in the queue?"

In addition to our own exploitation problems at NSA, we must also improve our man-machine interfaces so that software can be written quickly to assist analysts in solving technical, analytic [redacted] problems so that field stations and remoted sites can be directed more intelligently toward collection of desired targets of known value, as opposed to available targets of unknown value. Our collection technology has far outstripped the old-fashioned collection manager who continually asked for all the activity an operator could find. The dialogue between collection manager and collector must improve to include steerage and guidance based on and driven by mechanical applications and techniques which force the machine to disgorge more than regurgitated machine formats of exactly what was forwarded by individual collectors.

In summary, we must learn the techniques of controlling our machines beyond just turning them on and watching them run and spit at us. We must direct them to help us do a better job of collecting desired targets, manipulating collection data, processing significant information, preparing reports quickly, disseminating needed information to selected customers rapidly, and feeding back to collection sites to refine the process regularly. This is not a simple task. But if we are going to exploit SIGINT sensibly in what is left of the twentieth century, the architecture for SIGINT Exploitation must address this part of the problem. In reality, it is not a new task. Stating requirements, establishing collection priorities, directing collection, analyzing and processing collection results, preparing and disseminating intelligence to identified customers, evaluating results and feeding back to field elements have been the basics of SIGINT Exploitation since before the waylaying of Greek messengers. The critical task before us is to master the modern and sophisticated tools of the trade to improve our efficiency in handling the constantly increasing flow of SIGINT, while avoiding and eliminating blockages that could lead rapidly to internal ruptures of the SIGINT Exploitation mechanism.

[redacted] we were introduced to the concept of hierarchical cluster analysis by the R51 CADRE team, whose program, PEP-1, purported to be a far more refined method of homogeneity testing than the traditional RYE program, XIBAR.

[redacted]

Note by [redacted]
CRYPTOLOG Cryptanalysis Editor:

XIBAR, a program written by Marjorie Mountjoy, has been resident on RYE for many years and has been the standard clustering program for NSA cryptanalysts. The preceding article by [redacted] by comparing the results from XIBAR and PEP-1, served as a reminder that CRYPTOLOG needed to have a look at R51's recent work on cluster analysis. I asked [redacted] for an article on PEP-1, and [redacted] responded to my plea with his article "A Little PEP Talk," which follows this note.

The main difference between XIBAR and PEP-1 lies in the manner in which thresholds are set. XIBAR uses a single threshold level which can either be program-computed or arbitrarily prescribed by the analyst. As the [redacted] article indicates, a change in the threshold by the analyst can cause a change in the XIBAR clustering. On the other hand, since the PEP-1 threshold levels are all computer-generated, they will produce the same clustering for all users. The sequence of thresholds derived by PEP-1 enables the analyst to obtain the entire subcluster structure of the input data in a single computer run.

[redacted] users can find operating instructions for PEP-1 in file GDOC. The references below contain descriptions of the different measures available in PEP-1, some examples of applications to Agency problems, and sample output.

References:

"Cluster Analysis: Introduction to Models and Methods," [redacted] *NSA Technical Journal*, Vol. XXII, No. 2, Spring 1977 (~~TSC~~).

"How to Cope with a Cluster Analysis Problem: The R51 Cluster Analysis Software Package," [redacted] *R51/PROG-NOTE/2/77*, 17 March 1977 (~~TSC~~).

"The Hierarchical Clustering of Cryptanalytic Data and Comparison with Multidimensional Scaling," [redacted] and [redacted] *NSA Technical Journal*, Vol. XXI, No. 4, Fall 1976 (~~TSC~~).

"An Application of Multidimensional Scaling and Cluster Analysis to a T12 Problem: Analyzing Similarity Matrices Produced by Human Perception and Judgment," [redacted] *R51/TECH/04/77*, 22 September 1977 (U).

~~SECRET//SI~~

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

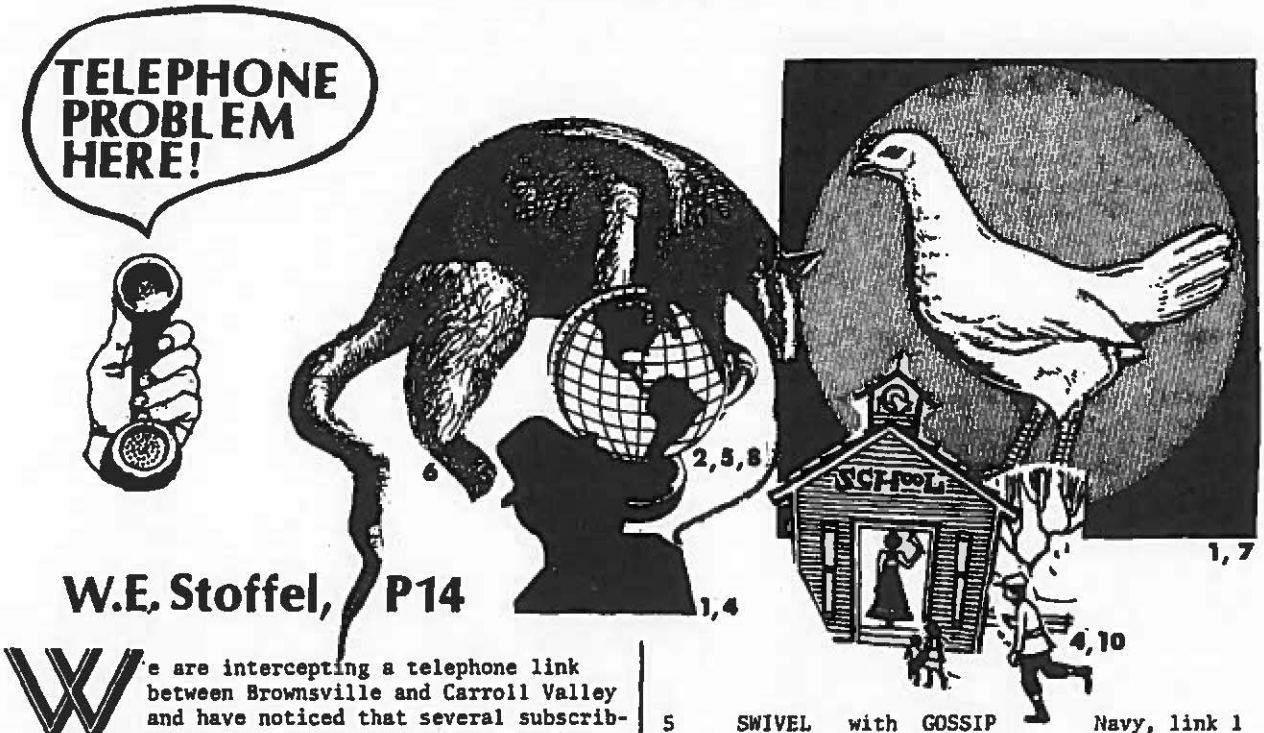
Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive



W.E. Stoffel, P14

We are intercepting a telephone link between Brownsville and Carroll Valley and have noticed that several subscribers are using covernames to disguise their identity. There are apparently five pairs of subscribers, three of whom are believed to be naval because of their speech patterns, and the other two are believed to be air-related. The covernames are apparently changing daily and, during the first 5 days, we have only been able to maintain continuity on one pair of subscribers. From the 6th on, we cannot distinguish the services, because the traffic has not yet been transcribed. Evidently the same covername can be used by two different people on the same day.

Date	*Brownsville*		*Carroll Valley*	*Identification*
1	MESA	with	OVAL	Navy, link 1
	APEMAN	"	CATBIRD	Navy
	BETA	"	TRANSOM	Navy
	PESO	"	SOLID	A/D
	SLUGGER	"	PULLET	A/D
2	VICTIM	with	ALBUM	Navy, link 1
	LOUVER	"	RIGGER	Navy
	MISFIT	"	GOSSIP	Navy
	SEEDLING	"	VALUE	A/D
	UNIT	"	SPHEROID	A/D
3	MYSTIQUE	with	LEATHER	Navy, link 1
	BULLY	"	SLUGGER	Navy
	TYPHOON	"	FIGHTER	Navy
	BETA	"	VICTIM	A/D
	TONIC	"	BLINKER	A/D
4	EQUAL	with	TRANSOM	Navy, link 1
	HATBOX	"	SCHOOLBOY	Navy
	REGENT	"	DISPLAY	Navy
	APEMAN	"	DISPLAY	A/D
	DICTION	"	BRACELET	A/D
5	SWIVEL	with	GOSSIP	Navy, link 1
	INTENT	"	QUENCHER	Navy
	SPHEROID	"	COUNTRY	Navy
	COUNTRY	"	HEXANE	A/D
	HATBOX	"	DOWNHILL	A/D
6	ADAGE	with	IMPULSE	--
	HYSSOP	"	PLODDER	
	MESA	"	HORMONE	
	AARDVARK	"	SLUGGER	
	GADGET	"	MISFIT	
7	CATBIRD	with	BARRETTE	--
	JUNGLE	"	DISPLAY	
	LINDEN	"	PULLET	
	LACEWING	"	CHASER	
	PROJECT	"	MORAY	
8	PILGRIM	with	SPHEROID	--
	RIGGER	"	MESA	
	SOLID	"	QUENCHER	
	THRESHOLD	"	QUENCHER	
	TONIC	"	ROWBOAT	
9	FIGHTER	with	VICTIM	--
	GADGET	"	IMPULSE	
	GERUND	"	COMPRESS	
	SEQUEL	"	VICTIM	
	VALUE	"	STACKER	
10	BLINKER	with	BULLY	--
	SCHOOLBOY	"	MYSTIQUE	
	SHILLING	"	CHASER	
	SINEW	"	PESO	
	TRANSOM	"	BRACELET	

Recover the continuities, system, and generation.

(Solution will appear next month.)

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive